UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DSIC DEPARTAMENT DE SISTEMES INFORMÀTICS I COMPUTACIÓ

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Dpto. de Sistemas Informáticos y Computación

Soberanía de datos: Un Análisis Comparativo de Conceptos y Prácticas en un Mundo Digital Globalizado

Trabajo Fin de Máster

Máster Universitario en Computación en la Nube y de Altas Prestaciones / Cloud and High-Performance Computing

AUTOR/A: Espinoza Solorzano, Roxana

Tutor/a: Bernabeu Aubán, José Manuel

CURSO ACADÉMICO: 2023/2024

Resumen

La noción de soberanía de los datos se refiere principalmente a la preservación del control y la gobernanza de los datos durante su recopilación, almacenamiento y procesamiento; esto se lleva a cabo de acuerdo con los marcos legales y las regulaciones que rigen una jurisdicción específica.

El principal desafío radica en la capacidad de asimilar la soberanía de los datos a los entornos tecnológicos a fin de establecer mecanismos eficaces para el intercambio y la regulación de la utilización de los datos, lo que exige un escrutinio continuo de los protocolos de seguridad de los datos.

Además, las complejidades de la globalización agravan este problema, particularmente en el ámbito de la computación en nube y el intercambio transnacional de datos, que implica la participación de naciones o estados, corporaciones e individuos.

Este documento busca enfrentar el desafío de analizar los marcos legales, las prácticas y las propuestas promulgadas para adherirse a la soberanía de los datos, con el objetivo de ofrecer pautas definitivas y consensuadas que faciliten el mantenimiento del control de los datos en un contexto digital global; esto abarca aspectos de privacidad, seguridad y gobernanza.

Palabras Claves: soberanía de datos, seguridad de datos, gobernanza en datos y leyes protección de datos.

Índice General

Resumen 2

Índice General 3

CAPÍTULO 1: INTRODUCCIÓN 7

1.1 Descripción de Problema 7

1.2 Motivación 8

1.3 Objetivos: 8

1.4 Impacto Esperado 9

1.5 Metodología Mixta 9

1.6 Estructura del documento 9

CAPÍTULO 2: FUNDAMENTO TEÓRICO 11

2.1 Definición y Alcance de Soberanía de Datos 11

Historia y evolución 11

Conceptualizando Soberanía de datos 13

2.2 Compendio de trabajos de investigación realizados 14

2.3 Conceptos Claves 46

Capítulo 3: Análisis de Marcos Legales y Regulatorios 54

3.1. Legislaciones Internacionales 54

3.2. Comparaciones de legislaciones 58

Capítulo 4: Implicaciones en la Seguridad y Privacidad de Datos 97

4.1 Análisis de Casos reales 97

4.1.1 Implicaciones para los Gobiernos 97

4.1.2 Implicaciones para las empresas 98

4.1.3 Implicaciones para los individuos 100

4.2. Cifras y Estadísticas 104

ESPAÑA 104

UNIÓN EUROPEA 105

EE.UU. Y REINO UNIDO 106
ESTADOS UNIDOS 107
4.3. Evaluación del impacto 107
4.3.1 Según los Principios Generales de la Protección de datos 107
4.3.2 Según las Garantías de Protección de Datos 110
Capítulo 5: Soluciones Tecnológicas para la Soberanía de datos 116
5.1 Infraestructura de Nube Soberana 120
5.1.1 Espacio de Datos: 120
5.1.2 Cooperativas de Datos: 122
5.2 Geofencing de Datos 124
5.3 Sistemas de Identificación Digital Nacionales 125
5.4 Soluciones de telecomunicaciones para la soberanía de datos 127
5.5 Tecnologías de Anonimización y Pseudonimización para el cumplimiento de la soberanía de datos 128
5.6 Blockchain para Trazabilidad y Cumplimiento 128
5.7 Plataformas para el cumplimiento de la soberanía de datos 128
5.8 Infraestructura de Clave Pública (PKI) para garantizar el cumplimiento de la soberanía de datos 129
5.9 Iniciativas para la soberanía de los datos sanitarios 130
5.10 Cifrado de Datos para el cumplimiento de la soberanía de datos 131
5.11 Software de apoyo al cumplimiento de leyes de soberanía de datos 132
Capítulo 6: Recomendaciones Prácticas 134
6.1 Directrices y Estrategias generales recomendadas: 134
6.2 Guías para implementación del cumplimiento de la soberanía de datos 135
6.2.1 Guías para Entidades Gubernamentales: 135
6.2.2 Guía para Corporaciones: 137
6.2.3 Guía para PYMES: 139
6.2.4 Guía para Individuos: 142
6.3 Validación 144
6.3.1 Listado de requisitos para integrar la soberanía de datos 144

6.3.2 Categorización de Requisitos:..... 148
6.3.3 Validación 149
6.3.4 Prueba 150
Capítulo 7: Conclusiones 152
7.1 Resumen de lo encontrado 152
7.2 Contribuciones 154
7.3 Limitaciones 155
7.4 Trabajos futuros 155
Referencias Bibliográficas 157
Referencias Web 164
Anexo 1: Leyes en países sobre Protección de Datos 174
Anexo 2: Reporte de FTC 195
Anexo 3: Requisitos funcionales y no funcionales..... 201
Anexo 4: Ejecución de Guía para Empresas..... 203

Índice de Tablas

TABLA 1: VALIDACIÓN DE ARTÍCULOS DE INVESTIGACIÓN Y AUTORES 15
TABLA 2: COMPARACIÓN DE ARTÍCULOS DE INVESTIGACIÓN CON RESPECTO A LA SOBERANÍA DE DATOS..... 16
TABLA 3: MATRIZ DE MARCOS LEGALES Y POLÍTICOS EN EL MUNDO DE SOBERANÍA DE DATOS 58
TABLA 4: CUADRO COMPARATIVO DE LAS SOLUCIONES TECNOLÓGICAS QUE SE INTEGRAN A LA SOBERANÍA DE DATOS..... 116
TABLA 5: CUADRO DE REQUERIMIENTOS VS. DOMINIOS..... 148
TABLA 6: RESULTADO DE EVALUACIÓN PARA EL CUMPLIMIENTO DE LA SOBERANÍA DE DATOS 150

Índice de ilustraciones

ILUSTRACIÓN 1: CRONOLOGÍA DE LA UTILIZACIÓN DE LA SOBERANÍA DE DATOS 12
ILUSTRACIÓN 2: ENFOQUES DE LA SOBERANÍA DE DATOS..... 14
ILUSTRACIÓN 3: MAPAMUNDI DE PAÍSES CON LEYES DE PRIVACIDAD DE DATOS 55

ILUSTRACIÓN 4: CANTIDAD DE PAÍSES POR CONTINENTE CON LEYES DE PRIVACIDAD DE DATOS 55
ILUSTRACIÓN 5: LOS PRINCIPALES ASPECTOS CONSIDERADOS PARA EL CUMPLIMIENTO DE LA SOBERANÍA DE DATOS 93
ILUSTRACIÓN 6: IMPLICACIONES DE LA SEGURIDAD Y PRIVACIDAD DE DATOS 103

CAPÍTULO 1: INTRODUCCIÓN

1.1 Descripción de Problema

En la era digital actual, la protección y el control de datos se ha convertido en una prioridad crítica para gobiernos, empresas y ciudadanos. El concepto de soberanía de datos, que se refiere a la capacidad de una entidad o individuo para controlar y regular los datos generados dentro de sus fronteras, está ganando cada vez más relevancia en el ámbito internacional según [20]. Este concepto se ha vuelto relevante en un mundo donde los datos fluyen a través de fronteras sin restricciones, y son utilizadas por una variedad de tecnologías innovadoras y establecidas nos comenta [62].

La soberanía de datos no solo implica la protección de los datos personales, sino también se extiende a diversos espacios de datos que incluyen datos educativos, de transporte, medioambientalista, de salud, financieros, de investigación, industriales, de identidad digital, telecomunicaciones, de seguridad pública, diferentes infraestructuras y entidades privadas y gubernamentales. [34] nos dice que todos estos espacios de datos presentando desafíos que requieren un enfoque integral y colaborativo para garantizar su protección y uso adecuado en beneficio de la sociedad en su conjunto.

En esta investigación nos centramos en los últimos cinco años, el motivo por el que se eligió este periodo es porque es un factor comúnmente utilizado para definir el “ciclo de vida de la tecnología” y esto se ve plasmado también en el uso de la soberanía de datos, la cual ha ganado una importancia especial en el desarrollo e implementación de varias soluciones tecnológicas, por ejemplo, la computación en la nube, Big Data y la inteligencia artificial las cuales han tenido que adaptarse a las nuevas regulaciones y estándares de la soberanía de datos. Para la computación en la nube, se sugiere y a veces impone que los proveedores de servicios garanticen la ubicación física de los datos dentro de ciertas fronteras geográficas específicas lo sugiere [49]. En la Big Data, la localización de datos y la implementación de la anonimización de información personal se han convertido en aspectos críticos a considerar para cumplir con las normativas de protección de datos vigentes en diferentes jurisdicciones lo destaca [27]. Asimismo, la inteligencia artificial también se ha visto afectada por estas regulaciones por los datos que alimentan sus modelos de entrenamiento y la protección de datos sensibles.

A la vez en muchas tecnologías se han incorporado los principios de soberanía de datos en sus frameworks como, por ejemplo: Internet de las Cosas (IoT), blockchain, edge computing, vehículos autónomos, realidad aumentada y virtual (AR/VR), redes 5G, biometría, sistemas de gestión de energía, telemedicina, drones, Fintech, robótica, y sistemas de gestión de identidad digital. Las mismas que se preocupan por los factores como el almacenamiento local, la protección de la privacidad, la seguridad de datos, el cumplimiento normativo y la reducción de la transferencia de datos transfronterizos.
Enfocaremos esta investigación al papel relevante que desempeña la soberanía de datos a la hora de permitir a las autoridades reguladoras crear un entorno de datos seguro que defienda los derechos y la privacidad de los ciudadanos, quienes son los que deben tener la soberanía de sus datos según nos indica [32]. Esta investigación se sumerge en la complejidad de los conceptos que rodean la soberanía de datos, explorando su evolución y cómo se ha adaptado a los desafíos de un entorno digital en constante cambio. Se comenzará por establecer una definición precisa de la noción de soberanía de datos, examinando los marcos legales y las regulaciones en varios países o regiones, el alcance de la seguridad y privacidad de los datos e investigando las soluciones tecnológicas que implementan o se esfuerzan por cumplir con las estipulaciones de la soberanía de los datos; en última instancia, se presentaran recomendaciones prácticas para las organizaciones. El objetivo es proporcionar información que facilite una comprensión integral y comparativa de la aplicación práctica de la soberanía de los datos en un entorno digitalizado.

1.2 Motivación

La integración de la soberanía de datos en los diferentes entornos tecnológicos de las organizaciones gubernamentales y privadas que garanticen la protección de la privacidad y seguridad de la información personal del individuo y promuevan la transparencia en el manejo de datos fomentando la confianza entre los ciudadanos y las instituciones.

1.3 Objetivos:

1.1.1 Proporcionar una mayor claridad del Concepto de Soberanía de Datos: Proporcionar una comprensión integral de qué es la soberanía de datos y su importancia en la era digital.

1.1.2 Analizar los Marcos Legales y Regulatorios: Examinar los marcos legales y regulatorios relacionados con la soberanía de datos en diferentes países y

regiones, incluyendo leyes de protección de datos y acuerdos internacionales. Comparar y contrastar las prácticas resaltando las diferencias y similitudes.

1.1.3 Evaluar las Implicaciones en la Seguridad y Privacidad de los Datos: Evaluar cómo las regulaciones de soberanía de datos impactan en la seguridad y privacidad de los datos, tanto para individuos como para organizaciones.

1.1.4 Explorar Soluciones Tecnológicas: Investigar soluciones tecnológicas que ayuden a las organizaciones a cumplir con los requisitos de soberanía de datos, como la cifra de datos, protocolos seguros de transferencia de datos y estrategias de localización en la nube.

1.1.5 Ofrecer Recomendaciones para el Cumplimiento de la Soberanía de Datos: Brindar recomendaciones prácticas para que las organizaciones puedan afrontar los desafíos del cumplimiento de la soberanía de datos y mantener la seguridad y privacidad de los datos.

1.4 Impacto Esperado

Contribuir al debate académico y práctico sobre la soberanía de datos, proporcionando una perspectiva analítica y constructiva, ofreciendo recomendaciones prácticas y aplicables para las organizaciones que buscan cumplir con las normativas y leyes existentes sobre soberanía de datos y proteger la información en un entorno digital complejo.

1.5 Metodología Mixta

Cualitativa (explorar conceptos, opiniones y experiencias), Documental (ayuda a construir una base sólida de conocimiento sobre la soberanía de datos y su contexto legal y regulatorio.) y Comparativa (Implica comparar y contrastar diferentes conceptos, objetos u otros).

1.6 Estructura del documento

Se ha estructurado el documento en siete capítulos:

En el Capítulo I, Se define los objetivos, la motivación, la metodología e impacto esperado del trabajo final del Máster.

En el Capítulo II, se desarrolla una comprensión integral de qué es la soberanía de datos; sintetizando las definiciones y perspectivas encontradas en la literatura y finalizando con una definición clara y coherente basada en tu revisión de la literatura.

En el Capítulo III, se examina los marcos legales y regulatorios en diferentes países y regiones; identificando las leyes y regulaciones en los países o regiones. Se realiza un análisis comparativo de estas leyes y regulaciones más relevantes.

En el Capítulo IV, se evalúa las implicaciones en Seguridad y Privacidad; se estudia los casos de empresas y organizaciones afectadas por estas regulaciones. Se analiza cómo estas regulaciones impactan la seguridad y privacidad de los datos.

En el Capítulo V, se investiga las soluciones tecnológicas para cumplir con los requisitos de soberanía de datos. Se identifica las tecnologías clave como cifrado de datos, protocolos seguros de transferencia y estrategias de localización en la nube. Se evalúa la efectividad de estas tecnologías en diferentes contextos.

En el Capítulo VI, se ofrecen recomendaciones prácticas para el cumplimiento de la soberanía de datos basado en los hallazgos de los análisis anteriores para desarrollar recomendaciones, considerando aspectos legales, técnicos y organizacionales. Proponiendo estrategias prácticas y viables para la implementación.

Finalmente, en el Capítulo VII, se resumen lo encontrado en la investigación, las contribuciones que realiza con el trabajo, las limitaciones que aún se tiene en este tema y los trabajos futuros que podrían seguir desarrollando.

CAPÍTULO 2: FUNDAMENTO TEÓRICO

2.1 Definición y Alcance de Soberanía de Datos

El concepto de soberanía de datos es complejo y evoluciona continuamente, especialmente en el contexto de esta era totalmente digital y globalizada; por esto organizaremos la información encontrada para dar una definición que englobe las diferentes ideas sobre este término.

Historia y evolución

En los 90, cuando internet comenzó a convertirse en una herramienta fundamental para la comunicación y el comercio; los datos personales y comerciales cruzaron fronteras físicas sin restricciones, empezando a preocupar a los gobiernos la pérdida del control de información de sus ciudadanos y empresas. Como respuesta a esta preocupación, surgieron debates sobre la necesidad de establecer regulaciones internacionales para proteger la privacidad y la seguridad de los datos en un mundo cada vez más interconectado.

En 1995 la Unión Europea (UE) tomo la iniciativa al adoptar la Directiva de Protección de Datos, la que establece los estándares mínimos para la privacidad y protección de datos de los Estados miembros. Esta iniciativa fue el primer intento de regular los flujos de datos dentro y fuera de Europa y ejercer el control sobre la soberanía de datos sugieren [32].

Iniciando el siglo XXI con la explosión de las grandes tecnologías y empresas mundiales como Google, Facebook, Amazon y Microsoft; la cantidad de datos generados y almacenado en sus propios servidores creció exponencialmente, estas empresas que en su mayoría tienen sus sedes principales en Estados Unidos comenzaron a dominar la información digital global, lo que permitió que ciertas leyes de este país concedan a las agencias gubernamentales acceder a los datos almacenados en su territorio nos comentan [2]. Por lo que esta concentración de datos planteó preocupaciones sobre la privacidad y la seguridad de la información personal de los usuarios, lo que llevó a un debate global sobre la necesidad de una regulación más estricta en el ámbito de la protección de datos.

Todo esto cobro más importancia en el 2013 con las revelaciones de Edward Snowden, quien expuso las extensas operaciones de vigilancia llevadas a cabo por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y otras agencias de inteligencia en colaboración con empresas tecnológicas. Este escándalo alertó a las autoridades de la

necesidad de revisar las leyes existentes y establecer mecanismos más transparentes para proteger la privacidad de los ciudadanos en la era digital, según lo indica [46].

[32] nos comentan que es así como en esta década de los 2010 empieza a surgir en varios países y regiones, normativas más estrictas en cuanto al manejo de datos personales y la supervisión de las actividades de vigilancia gubernamental, con el objetivo de garantizar la privacidad y seguridad de los individuos en línea. De nuevo liderando este esfuerza la Unión Europea en el 2018 implemento el Reglamento General de Protección de Datos (GDPR). Paralelamente, China implementó en el 2017 su Ley de Ciberseguridad según [58] y Rusia también adoptó leyes que exigen el control de los datos personales de sus ciudadanos según [26]. Mientras que en Estados Unidos específicamente en el estado de California se promulgó la Ley de Privacidad del Consumidor de California (CCPA) en 2018, que establece regulaciones similares a las del GDPR europeo, pero con algunas diferencias clave en cuanto a la protección de datos personales nos señala [5]. A continuación, se muestra la línea cronológica en la Ilustración 1, de los hitos de la soberanía de datos:

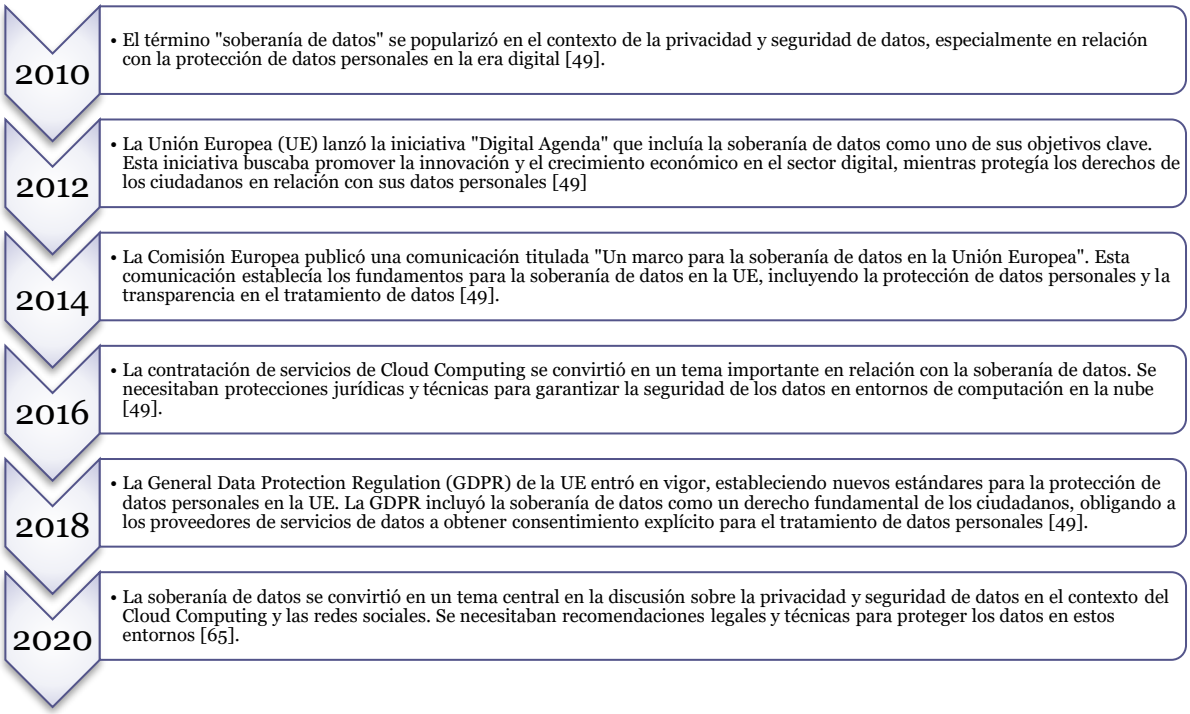

ILUSTRACIÓN 1: CRONOLOGÍA DE LA UTILIZACIÓN DE LA SOBERANÍA DE DATOS

Conceptualizando Soberanía de datos

La soberanía de los datos es un concepto que abarca múltiples disciplinas y se examina desde varias perspectivas teóricas. Estas perspectivas se utilizarán para elaborar una definición integral que abarque las investigaciones realizadas en los últimos cinco años. Este plazo coincide con la introducción del GDPR el 25 de mayo de 2018, que constituye un punto importante desde el que comenzar a explorar las investigaciones pertinentes sobre este tema en particular.

Los marcos teóricos a través de los cuales se sugiere definir la soberanía de los datos son los siguientes:

Para un ***enfoque sociotécnico,*** la soberanía de datos es una extensión esencial de la soberanía estatal en la era digital, adaptándose a los desafíos y oportunidades que presenta el ciberespacio. Este concepto continúa evolucionando a medida que las tecnologías avanzan y las interacciones digitales se vuelven cada vez más integrales en nuestras vidas cotidianas [3].

Para un ***enfoque de los derechos humanos,*** la soberanía de datos es un concepto multidimensional que abarca el control, la propiedad y los derechos sobre los datos. Es crucial para asegurar que los datos se manejen de manera ética y conforme a los derechos y valores de los sujetos de datos [32].

Para un ***enfoque económico,*** la soberanía de datos es un concepto esencial en la era digital, donde el control sobre la información y los datos es crucial para la seguridad nacional, la privacidad y la competitividad económica. La relación entre los estados soberanos y las grandes empresas tecnológicas es compleja y requiere una regulación cuidadosa para asegurar que los datos se manejen de manera ética y conforme a los intereses nacionales. En el contexto moderno, este control es esencial debido a la creciente importancia de los datos en la economía y la política globales [27].

Para un ***enfoque político,*** la soberanía de datos propone una definición que extiende las nociones tradicionales de control estatal al ámbito digital, donde los datos se consideran un activo fundamental que debe regirse y protegerse mediante leyes y políticas nacionales; garantizando el cumplimiento de las leyes nacionales, protegiendo la privacidad y la seguridad; sin dejar de participar en la economía digital global [33].

Para un ***enfoque legal,*** la soberanía de datos abarca el control y la autoridad sobre los datos a nivel individual, organizacional y estatal, asegurando que estos se manejen de acuerdo con las leyes y regulaciones locales y protegiendo así la privacidad y los derechos de los datos [16].

Para un ***enfoque ético,*** la soberanía de datos se define como un concepto integral que incluye el control, la autoridad y el poder de toma de decisiones sobre los datos, enmarcado en el contexto de un contrato social para garantizar que las prácticas de datos estén alineadas con el bien colectivo y los estándares éticos de la sociedad [2].

Para un ***enfoque de la gobernanza de datos,*** se define la soberanía de los datos como el cumplimiento de las leyes y estructuras de gobierno locales en relación con los datos recopilados y procesados en un país, destacando su importancia para proteger la privacidad y la confianza de los usuarios y proponiendo un marco para ayudar a las empresas a garantizar el cumplimiento de estas leyes [54].

Resumiendo, como podemos ver en la Ilustración 2 la soberanía de datos tiene 7 bloques principales.

ILUSTRACIÓN 2: ENFOQUES DE LA SOBERANÍA DE DATOS

2.2 Compendio de trabajos de investigación realizados

En esta sección en particular, se analizará en profundidad los antecedentes históricos y los principales esfuerzos de investigación relacionados con la soberanía de los datos. Para lograr este objetivo, el primer paso consiste en identificar los estudios más pertinentes, teniendo en cuenta la frecuencia de citas atribuida a cada obra y el cálculo del índice «h», que significa el número de publicaciones que superan un cierto umbral de citas. Este proceso arroja luz sobre el impacto del autor en este campo. A

continuación, se proporciona un cuadro completo (ver Tabla 1) que ilustra los criterios de validación antes mencionados para una comprensión más clara del panorama de la investigación en el ámbito de la soberanía de los datos.

TABLA 1: VALIDACIÓN DE ARTÍCULOS DE INVESTIGACIÓN Y AUTORES

Nro.	Nombre del Documento	Citados	Autor	Citado 2019	Índice h
1	The European Union general data protection regulation: what it is and what it means	552	Chris Jay Hoofnagle	2347	23
2	What does the notion of “sovereignty” mean when referring to the digital?	300	Sophie Toupin	593	9
3	Digital sovereignty	298	Julia Pohle	750	12
4	The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU	288	Luciano Floridi	41013	87
5	Data sovereignty: A review	251	Patrick Hummel	867	12
6	Data sovereignty and data space ecosystems	92	Matthias Jarke	9628	34
7	Safeguarding European values with digital sovereignty: an analysis of statements and policies	92	Huw Roberts	1164	9
8	Contested Spatialities of Digital Sovereignty	68	Georg Glasze	1890	22
9	Usage control architecture options for data sovereignty in business ecosystems	61	Boris Otto	9428	42
10	Data Co-Operatives through Data Sovereignty	55	Igor Calzada	3166	27
11	Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity	46	Benjamin Farrand	385	10
12	Artificial intelligence and EU security: the false promise of digital sovereignty	45	Andrea Calderaro	328	7
13	Data Sovereignty and the Internet of Production	37	Matthias Jarke	9628	34

14	On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications	34	Christian Esposito	4260	32
15	A Delimitation of Data Sovereignty from Digital and Technological Sovereignty.	15	Malte Hellmeier	42	4
16	Implementing Data Sovereignty: Requirements & Challenges from Practice	9	Malte Hellmeier	42	4
17	Data sovereignty for AI pipelines: lessons learned from an industrial project at Mondragon corporation	9	Julia Pampus	46	4
18	Data sovereignty in information systems	7	Malte Hellmeier	42	4
19*	Beyond control over data: Conceptualizing data sovereignty from a social contract perspective	0	Antragama Ewa Abbas	237	8
20*	An Empirical Examination of the Technical Aspects of Data Sovereignty	0	Julia Pampus	46	4

(*****) Los artículos de investigación más recientes, los números 19 (publicados en enero de 2024) y 20 (presentados en la 19ª Conferencia Internacional sobre Tecnologías del Software en julio de 2024), no incluyen citas debido a su reciente publicación, pero los autores, son muy conocidos en el campo, tienen un índice h respetable.

El cuadro comparativo (ver tabla 2) que se presenta a continuación ofrece datos relevantes y valiosos extraídos de los trabajos de investigación mencionados anteriormente, resumiendo sucintamente las principales consultas realizadas durante el curso de los estudios:

TABLA 2: COMPARACIÓN DE ARTÍCULOS DE INVESTIGACIÓN CON RESPECTO A LA SOBERANÍA DE DATOS

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
1	The European Union general data protection regulation: what it is and what it means [31].	Legal	• Análisis comparativo. • Consulta bibliográfica.	• Explicación del GDPR de manera comprensible y sencilla para ser entendida por cualquiera interesado en usarla. • Análisis sistemático desde todos los ángulos (histórico, estratégico, normativo, asignación de roles y responsabilidades, nivel de cumplimiento y penalización). • Plantea formas para lograr el cumplimiento del GDPR, incentivando la gobernanza de datos.	• La complejidad de este reglamento puede dificultar el cumplimiento de las pequeñas y medianas empresas. • Algunas de las disposiciones del GDPR están redactadas a un nivel de principios más que de reglas específicas. • El problema que pueda ocasionar en el mercado de datos ocasionando el desaliento de las	El uso del GDPR principalmente contribuye al cumplimiento de la protección y control de los datos personales dentro de la Unión Europea, lo cual es el principio fundamental de la soberanía de datos.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					inversiones para los sectores tecnológicos.	
2	What does the notion of “sovereignty” mean when referring to the digital? (Stéphane Couture et al., 2019)	Ético	• Búsqueda bibliográfica • Análisis de publicaciones.	• Estudiar el concepto de “soberanía” para el mundo digital. • La noción de soberanía digital depende de los actores y sus propios objetivos y conceptualizaciones. • Enfoque de análisis de los diversos usos de soberanía especialmente en los estados y otros niveles de organizaciones colectivas, movimientos sociales y pueblos indígenas. • Se sitúa en el contexto histórico y epistemológico de la soberanía que va desde el control colectivo	• Limitada generalización debido a que se centra en grupos activistas y tecnología específicos. • Pasa por alto las perspectivas no occidentales y simplifica el complejo concepto de soberanía.	La soberanía de los datos se define como "el intento de los Estados-nación de someter los flujos de datos a jurisdicciones nacionales". Se distinguen dos tipos: la soberanía débil y la soberanía fuerte. La soberanía débil se refiere a iniciativas lideradas por el sector privado, centradas en la protección de derechos digitales, mientras que la soberanía fuerte es un enfoque estatal orientado a

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				hasta la autonomía individual.		salvaguardar la seguridad nacional.
3	Digital sovereignty (Pohle & Thiel, 2020)	Gobernanza de datos	• Revisión de la literatura. • Análisis conceptual. • Estudios de casos.	• Resurgimiento de la soberanía estatal, los estados se están adaptando al ámbito digital. • Inclusión de autonomía estatal, económica y autodeterminación individual en el concepto de soberanía digital. • Enfoque en la protección de infraestructuras críticas y la gestión de datos dentro de fronteras nacionales. • Esfuerzos para reducir la dependencia tecnológica extranjera y promover la innovación local, ejemplificados por iniciativas como GAIA-X.	• No hay datos que respalden sus afirmaciones. • El contexto se limita a la realidad europea. • Falta de ejemplos implementados para cumplir con los desafíos. • No se describe alguna propuesta que pueda implementarse. • No toma en cuenta los desafíos prácticos y políticos. • No logra profundizar de como lograra la legitimidad y aceptación popular.	• Sugiere medidas concretas como la localización de datos y el proyecto GAIA-X para reforzar la soberanía de datos. • Propone reafirmar la autoridad estatal, abordar la protección de los bienes vitales, responder a las prácticas de vigilancia, hacer hincapié en la gobernanza política, destacar los desafíos y los riesgos, abogar por la rendición de cuentas democrática y sistematizar las

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				• Protección de los derechos de los usuarios y fomento de la capacidad de decisión informada sobre el uso de tecnologías digitales. • Uso de la soberanía digital como práctica discursiva en la política para justificar la intervención estatal en el ámbito digital. • Mejora de la alfabetización digital del ciudadano que incluya un compromiso crítico de la tecnología y los datos.		diversas reivindicaciones de soberanía digital.
4	The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU (Floridi, 2020)	Gobernanza de datos	Análisis conceptual y teórico.	• Explica por qué la soberanía digital es de importancia universal (controlar los datos, software, estándares, procesos, servicios, infraestructuras, etc.) • Compara ejemplos recientes como la soberanía digital es	• No hay suficiente evidencia cuantitativa. • El enfoque solo centra en la UE. • No hay propuestas específicas de directrices para	• Propone una estructura supranacional para una respuesta coordinada a los desafíos de la soberanía digital.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				crítica para los países y grandes empresas tecnológicas. • La dinámica de los Estados y las Empresas tecnológicas, en donde existe dependencia del Estado y a la vez este intenta regular su uso y control de la tecnología digital. • La necesidad de la soberanía digital supranacional. • Propone un modelo de gobernanza basado en un híbrido de red que incluya todos los niveles de soberanía (popular, nacional y Supranacional) para un control democrático y efectivo.	implementar la propuesta. • No se profundiza como lograr el apoyo público y político.	• Propone un modelo de gobernanza que combina los niveles de soberanía. • Resalta la importancia de la soberanía digital para proteger la privacidad y los datos de los ciudadanos.
5	Data sovereignty: A review [32].	Derechos humanos	• Revisión sistemática.	• El documento presenta una cuadrícula conceptual para	• Alcance limitado a la escritura académica,	El desarrollo de un marco conceptual que

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
			• Desarrollo inductivo. • Análisis cualitativo.	sistematizar los diversos significados candidatos de la soberanía de los datos. • La soberanía de los datos puede aplicarse a una variedad de agentes, desde individuos hasta sociedades y países enteros. • La soberanía de los datos se discute principalmente en el contexto de la arquitectura de TI y las leyes de procesamiento de datos, pero también en otros contextos, y tiende a abordar una mezcla matizada de valores relacionados con el control, el poder, la deliberación inclusiva y los derechos fundamentales.	no incluye otros dominios como el periodismo o las redes sociales. • No evalúa la idoneidad de las estrategias para promover la soberanía de los datos en la práctica. • Se utilizan conceptos amplios que no están definidos uniformemente en la literatura.	clasifica las diferentes dimensiones de la soberanía de datos, en: Agente implicado, dominios o contexto, valores normativos, enfoques, desafíos, estrategias de gestión, menciones y entendimientos, evaluación e implementación y cuestiones prácticas.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
6	Data sovereignty and data space ecosystems [36].	Sociotécnico	Análisis Experimental	• Las organizaciones necesitan acceder y utilizar datos de fuentes externas, más allá de los datos internos y públicos, para seguir siendo competitivas. • Se están utilizando diversas tecnologías para permitir el intercambio y la compartición de datos, como el mapeo de datos, la transformación, el procesamiento paralelo, el aprendizaje automático y la cadena de bloques. • El concepto de "soberanía de datos" y "ecosistemas de datos impulsados por alianzas" ha surgido como una forma de permitir el intercambio y la compartición de datos, y la Asociación Internacional del Espacio de	• Dependencia de plataformas dominantes, esto puede limitar la competitividad y la capacidad de las organizaciones más pequeñas o nuevas para participar equitativamente en los ecosistemas de datos. • La reutilización de datos para propósitos diferentes a los originalmente previstos puede generar problemas de calidad. • Aunque se propone el uso de modelos de privacidad diferencial,	El aporte a la soberanía de datos se centra en la creación y gestión de ecosistemas de espacios de datos. Estos ecosistemas permiten a las organizaciones y a los individuos mantener el control sobre sus datos, asegurando que se manejen de acuerdo con sus propias políticas y regulaciones. Destaca la importancia de estos ecosistemas para facilitar la interoperabilidad y la colaboración entre diferentes entidades,

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				Datos está desarrollando una arquitectura de referencia para dichas plataformas.	la implementación efectiva de estas técnicas en escenarios reales puede ser compleja y no siempre garantiza una protección total. • Los ecosistemas de datos colaborativos están en una etapa relativamente temprana. • La implementación práctica de la soberanía de datos requiere marcos regulatorios y tecnológicos robustos que aún están en desarrollo.	mientras se preserva la soberanía de los datos.
7	Safeguarding European values	Gobernanza de datos.	• Revisión de Literatura.	• Conceptualizar la definición de soberanía digital.	• Falta de una definición clara del	• El documento identifica el concepto

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
	with digital sovereignty: an analysis of statements and policies [47].		• Análisis Conceptual. • Recolección y Análisis de datos.	• Análisis Empírico que definió cinco áreas clave: Gobernanza de datos, Limitación del Poder de las Plataformas, Infraestructuras digitales, Tecnologías emergentes y Ciberseguridad. • Análisis de la eficacia de las políticas actuales implementadas por la UE. • Propuestas de pasos y recomendaciones para mejorar la soberanía digital en la UE.	término “soberanía digital”, lo que obstaculiza la capacidad de desarrollar una agenda política coherente. • La agenda de soberanía digital de la UE se ve socavada actualmente por las limitaciones percibidas de la legitimidad de sus procesos de formulación de políticas. Esto puede conducir a resultados poco éticos si la UE no es capaz de introducir medidas reguladoras	de la soberanía digital y como se relaciona con la gobernanza de datos. • Ofrece recomendaciones prácticas: comprensión común y coherente en toda la UE; fortalecer el alcance global de la UE y apoyar a las empresas tecnológicas en la UE y mejorar la legitimidad y transparencia de los procesos de toma de decisiones de la UE.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					suficientemente sólidas. • Las grandes empresas de tecnología ejercen un considerable control de facto sobre varios aspectos de la vida digital, lo que puede socavar los esfuerzos de la UE. • La UE se enfrenta a un delicado equilibrio entre mantener la apertura y la cooperación internacional y proteger sus intereses digitales. Este equilibrio puede llevar a compromisos que pueden diluir la	

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					eficacia de las medidas de soberanía digital.	
8	Contested Spatialities of Digital Sovereignty [26].	Político	• Análisis comparativo. • Estudios de caso. • Talleres colaborativos.	• Recolección de aportes realizados de los ensayos presentados en el foro geopolítico descrito en el Título. • La geopolitización de los flujos de datos se refiere a la creciente importancia de los datos ha transformado la geopolítica digital, con los estados compitiendo por el control de la información y estableciendo nuevas fronteras digitales para proteger sus intereses nacionales. • El artículo explora enfoques opuestos de la soberanía digital, con Rusia	• El campo de la soberanía digital está evolucionando rápidamente y este artículo se basa en talleres realizados en 2020 y 2021, es posible que algunos de los hallazgos ya no reflejen completamente la situación actual. • No ofrece suficientes soluciones prácticas o estrategias viables para que los responsables políticos y las partes interesadas aborden	El compendio contribuye significativamente al entendimiento de la soberanía de datos al analizar cómo se configura y disputa en diferentes contextos geopolíticos, y cómo las prácticas y discursos de soberanía digital reflejan y producen nuevas espacialidades y relaciones de poder en el ámbito digital.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				persiguiendo el aislamiento y la UE tratando de equilibrar el control con la apertura. Además, se realizan otras comparaciones con los Estados Unidos y China actores principales y otros países que tratan de ir a la par de los desafíos de la soberanía digital. • Identificación de estrategias para fortalecer la soberanía digital, como leyes de localización de datos y nubes soberanas. • El documento analiza los desafíos que plantean las interacciones digitales transfronterizas, como la computación en nube y las plataformas digitales, que requieren nuevas formas de	estos desafíos de manera efectiva. • El artículo hace hincapié en el análisis y el discurso teóricos, que podrían no ser tan útiles para los profesionales que buscan ejemplos concretos y mejores prácticas para implementar en sus propias iniciativas de soberanía digita	

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				cooperación y regulación internacionales para garantizar la seguridad y la privacidad de los datos.		
9	Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity [20].	Político	Análisis cualitativo	• La UE está pasando de un modelo de "Capitalismo Regulatorio" a uno de "Mercantilismo Regulatorio" en su enfoque de ciberseguridad. • Reducción de la dependencia de actores privados externos. • La UE está haciendo una distinción entre empresas tecnológicas europeas (considerados socios confiables) y no europeas (vistas como posibles amenazas). • El artículo argumenta que la UE está adoptando un enfoque más proteccionista	• Dependencia significativa de un enfoque teórico y conceptual sin suficientes datos empíricos específicos. • Comparación insuficiente con políticas de soberanía digital y ciberseguridad de otras regiones del mundo. • Interpretación subjetiva de políticas y discursos sin	El artículo contribuye a la comprensión de la soberanía de datos al proponer un nuevo marco conceptual (Mercantilismo Regulatorio) que explica cómo la UE está buscando ejercer mayor control sobre sus datos y recursos digitales, redefiniendo su relación con el sector privado en el proceso.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				y centrado en el control estatal en su gobernanza de la ciberseguridad, redefiniendo su relación con el sector privado en el proceso.	validación empírica robusta.	
10	Data Co-Operatives through Data Sovereignty [13].	Sociotécnico	• Revisión bibliográfica. • Análisis de estudios de casos.	• El uso de cooperativas de datos para validar el uso de la soberanía de datos. • El uso práctico de la soberanía de datos en las “ciudades inteligentes centradas en las personas”. • Definición de dimensiones tecno-políticas y de Ciudad-Región, para construir un marco conceptual.	• Las cooperativas de datos aún están en un estado experimental. • Hay poca literatura académica que sea específica para la dimensión ciudad-región. • Las cooperativas de datos no son fáciles de replicar o ser usadas. • Falta de indicaciones claras para la federalización de los datos a través de los	Construcción de un marco conceptual que integre los conceptos de cooperativas de datos, el uso práctico de la soberanía de datos, la devolución de la data y el colonialismo de la data; esto dentro de las dimensiones Tecno políticas y Ciudad-Región centrándose en las “ciudades inteligentes centradas en las personas”, que

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					ecosistemas estados-nación.	consideran tanto el lado sociopolítico y socioeconómico digital.
11	Artificial intelligence and EU security: the false promise of digital sovereignty [12].	Política	Conceptual y analítico	• El documento encuentra discrepancias entre el enfoque normativo y legislativo de la UE para proteger su mercado digital y los pasos prácticos adoptados para desarrollar el liderazgo global de la UE en IA, destacando las tensiones internas en la comprensión de la UE de la soberanía digital. • La UE está a la zaga de EE. UU. y China en inversiones globales en IA y en la industria de seguridad/defensa, y la Brújula Estratégica de la UE no proporciona una visión	• Falta de herramientas y capacidades en las dimensiones clave de la IA (datos, algoritmos, hardware) en comparación con EE. UU. y China. • Falta de una industria tecnológica digital importante e inversiones insuficientes en IA en comparación con EE. UU. y China. • Falta de una estrategia de defensa consistente, a	Define la soberanía en IA en términos de control sobre datos, algoritmos y hardware, resaltando la falta de liderazgo de la UE en estos aspectos.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				clara para el desarrollo estratégico de la IA. • La UE carece de las herramientas necesarias, incluidas las inversiones, una industria tecnológica líder y una estrategia de defensa coherente, para lograr su objetivo anunciado de convertirse en un líder global en IA y alcanzar la soberanía digital.	diferencia de EE. UU. y China.	
12	Data Sovereignty and the Internet of Production [35].	Sociotécnico	• Análisis documental y experimental.	• El documento identifica una falta de conceptos coherentes para que las PYME e industrias con uso intensivo de conocimiento protejan sus datos y conocimientos en ecosistemas globalizados. • El documento propone una nueva abstracción de datos llamada "Sombras digitales"	• Falta una base legal para las PYMES. • No se presenta directrices prácticas y detalladas. • Generalización limitada al presentar su caso de uso.	Analizar el concepto de "soberanía de los datos" y los desafíos que afrontan las PYME y las industrias en Europa a la hora de proteger sus datos y conocimientos basados en modelos, en particular en el

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				para abordar los desafíos en el apoyo a enfoques basados en modelos y datos, siendo pequeña y móvil, ejecutable en tiempo real y adecuada para el intercambio controlado de datos. • El documento sugiere que construir un gemelo digital completo no es factible para el complejo entorno de "Internet de la producción", y el concepto de Sombras digitales se presenta como una solución.		complejo sector de producción.
13	On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications [18].	Sociotécnico	Análisis experimental.	• Propuesta de un enfoque criptográfico de dos niveles basado en la ubicación; este integra una capa adicional de encriptación a los mecanismos de seguridad existente para salvaguardar	• Determinar con precisión la ubicación geográfica de los usuarios y los dispositivos, lo cual es crucial para restringir	El documento propone de un enfoque criptográfico basado en la ubicación que integra métodos avanzados de encriptación y

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				los datos en la nube y la comunicación entre dispositivos del Internet de las Cosas (IoT) dentro de la infraestructura de una ciudad inteligente. • Método de localización para localizar usuarios en la nube y dispositivos IoT. • Se implementó un esquema ABE (encriptación basada en atributos) para restringir la accesibilidad de los datos dentro de áreas geográficas específicas. • La solución propuesta se adaptó para usar identificadores de ubicación en lugar de coordenadas geográficas, haciéndola más aplicable en contextos de ciudades inteligentes.	el acceso a los datos a áreas específicas. • La complejidad de la gestión de claves criptográficas aumenta con el número de usuarios y dispositivos. • Problemas de escalabilidad pueden surgir en grandes infraestructuras de ciudades inteligentes. • Requiere una infraestructura avanzada y robusta, lo que puede ser costoso y complejo. • La diversidad de regulaciones de protección de datos en diferentes jurisdicciones puede	localización para asegurar la soberanía de datos en aplicaciones de ciudades inteligentes. Esta solución permite un control más preciso sobre dónde y cómo se pueden acceder a los datos, abordando así las preocupaciones de seguridad y privacidad asociadas con el uso de la nube y dispositivos IoT en entornos urbanos.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				• El enfoque propuesto aborda eficazmente los desafíos de soberanía de datos tanto en entornos de nube como de IoT, permitiendo un mayor control sobre dónde se pueden acceder y utilizar los datos.	complicar la implementación.	
14	A Delimitation of Data Sovereignty from Digital and Technological Sovereignty [28].	Sociotécnico	Revisión sistemática de publicaciones académicas.	• La soberanía de los datos es el concepto más comúnmente discutido, centrándose en la capacidad de las personas y las organizaciones para controlar sus propios datos. • La soberanía digital se ocupa del control político y económico sobre las tecnologías e infraestructuras digitales, así como de permitir que las personas y las empresas utilicen los activos	• Los términos de búsqueda se centraron únicamente en la soberanía de datos, digital y tecnológica, y no consideraron conceptos relacionados como la protección de datos, la propiedad y el control de acceso. • La distribución de la literatura estuvo fuertemente sesgada	El artículo proporciona una delimitación de la soberanía de datos de la soberanía digital y tecnológica, mostrando que los conceptos se centran en diferentes dominios y tienen fuertes relaciones que se influyen entre sí, con implicaciones tanto para la teoría como para la práctica.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				digitales de manera interoperable. • La soberanía tecnológica es el concepto más amplio, centrándose en el control político e internacional sobre los recursos y capacidades tecnológicas, que a su vez influye en el desarrollo de sistemas de soberanía de datos.	hacia Europa, con una subrepresentación de otras regiones como África, Australia y Sudamérica. • El estudio no exploró el vínculo entre los conceptos de soberanía y los objetivos de sostenibilidad. • No está claro si los modelos de soberanía de datos se pueden crear independientemente de la soberanía digital y tecnológica.	
15	Implementing data sovereignty: Requirements &	Sociotécnico	Análisis Experimental	• El documento identificó 7 requisitos clave y 13 desafíos clave para implementar la soberanía de datos en la	• Posibles distinciones personales debido a que varios investigadores	El documento amplía las perspectivas teóricas y legislativas existentes sobre la

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
	challenges from practice [29].			práctica, que abarcan aspectos organizacionales, técnicos, personales y emocionales. • Los requisitos incluyen el cumplimiento legal/regulatorio, la clasificación de datos, la aplicación de políticas y la transparencia. • Los desafíos incluyen cuestiones legales/regulatorias, limitaciones técnicas y barreras organizacionales/culturales.	realizaron y analizaron las entrevistas. • Posibles restricciones a los participantes debido a su relación laboral. • Generalización limitada debido al pequeño tamaño de la muestra de 11 participantes. • Falta de diversidad en el grupo de participantes, ya que todos los entrevistados estaban radicados en Europa y tenían experiencia en soberanía de datos	soberanía de los datos con ideas prácticas. Este enfoque ayuda a cerrar la brecha entre la teoría y la práctica, y ofrece información valiosa tanto para los investigadores como para los profesionales
16	Data Sovereignty for AI Pipelines: Lessons Learned	Sociotécnico	Investigativa y Experimental.	Los hallazgos principales del documento son las diez lecciones aprendidas, cuatro	• Sesgo organizacional debido a que el estudio se realizó	El documento presenta las lecciones clave aprendidas, los

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
	from an Industrial Project at Mondragon Corporation [4].			beneficios y tres barreras para la implementación de canales de IA con soberanía de datos, que abordan las preguntas de investigación sobre las prácticas, los beneficios y las barreras de la soberanía de datos en los canales de IA.	dentro de una sola organización (Mondragón). • Validez externa limitada, ya que la solución y los hallazgos pueden parecer diferentes en otros contextos (por ejemplo, empresas más pequeñas, diferentes industrias). • Subjetividad en el proceso de reflexión y síntesis de los hallazgos, lo que podría llevar a conclusiones diferentes por parte de otros investigadores. • La necesidad de más estudios empíricos en	beneficios y las barreras para la implementación de canales de IA con soberanía de datos basados en un proyecto de investigación de acción de 12 meses con Mondragon Corporation.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					otros contextos para superar estas limitaciones y hacer avanzar los hallazgos hacia patrones de diseño más concretos	
17	Data Sovereignty in Information Systems [63].	Gobernanza de datos	Revisión de la literatura	• El documento propone un modelo conceptual para la soberanía de los datos en la investigación de Sistemas de Información, que consta de siete aspectos centrales que incluyen activos de datos, proveedores de datos, consumidores de datos, acuerdos contractuales, cadena de valor de los datos y actividades del ciclo de vida, infraestructura de datos y confianza. • El modelo conceptual se basa en la teoría de la agencia y	• El análisis de la literatura tiene limitaciones, ya que el uso de diferentes bases de datos o búsquedas podría llevar a diferentes resultados. • El enfoque de la teoría de la agencia utilizado para fundamentar el modelo conceptual tiene limitaciones, ya que está más estrechamente relacionado con el	Los autores presentan un modelo conceptual básico que incluye siete aspectos clave, como la confianza entre los proveedores de datos y los consumidores, la infraestructura de datos y los acuerdos contractuales, que interactúan para respaldar la soberanía de los datos durante todo el ciclo de vida de los datos

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				tiene como objetivo proporcionar una comprensión holística de la soberanía de los datos para guiar tanto a los investigadores como a los profesionales. • El modelo se valida a través de ejemplos del mundo real de la industria automotriz alemana y el monitoreo colaborativo de condiciones en empresas industriales.	área de Sistemas de Información definida "como un sistema en varias organizaciones". • El documento sugiere varias oportunidades de investigación futuras, incluido el examen del desarrollo necesario de artefactos para ayudar a las personas a controlar sus datos, la identificación de las capacidades necesarias para implementar la soberanía de datos como un instrumento y la exploración de la relación entre el valor	

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					de los datos, la economía de los datos y la soberanía de los datos.	
18	Beyond control over data: Conceptualizing data sovereignty from a social contract perspective [2].	Gobernanza de datos	Análisis cualitativo	• El estudio propone un marco conceptual multifacético de la soberanía de los datos que identifica aspectos clave más allá del mero control, como la privacidad, la propiedad, la seguridad, el cumplimiento y la responsabilidad • El marco proporciona una comprensión más integral de la soberanía de los datos y sienta las bases para un mayor desarrollo teórico en esta área. • Los hallazgos resaltan la importancia de considerar múltiples facetas de la soberanía de los datos, en	• El estudio se centra en la perspectiva del proveedor de datos, y las investigaciones futuras podrían explorar la perspectiva del consumidor de datos para obtener una visión más equilibrada. • La aplicabilidad del marco propuesto a otros entornos de intercambio de datos empresariales (jerarquía y modo de red) debe confirmarse empíricamente.	• Proponen un marco para la soberanía de los datos que incluye tres partes principales: protección, participación y provisión. • La parte de protección se centra en derechos básicos como la propiedad de los datos, lo que significa que las personas deben tener derecho a ser propietarias de sus datos y a decidir cómo se utilizan.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
				lugar de centrarse solo en el control, para evitar visiones reduccionistas.	• Los estudios cuantitativos futuros podrían fortalecer la validez nomológica del marco. • No se pretende que las condiciones contextuales identificadas sean exhaustivas, y existe la oportunidad de realizar una mayor exploración. • Ampliar el horizonte temporal para incluir períodos de cambios o eventos políticos significativos podría proporcionar información adicional.	• La parte de participación implica dividir las responsabilidades entre las diferentes partes para garantizar que los datos se usen y compartan de manera justa y responsable. La parte de provisión incluye mecanismos como el control, la seguridad y el cumplimiento para garantizar que los derechos básicos estén protegidos cuando se comparten datos.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
19	An Empirical Examination of the Technical Aspects of Data Sovereignty [43].	Sociotécnico	Análisis cualitativo	• La capacidad de los participantes que comparten datos para modificar los flujos de datos es un requisito fundamental para la soberanía de los datos. • La seguridad y la confiabilidad del sistema son fundamentales para permitir la soberanía de los datos. • La interoperabilidad, la capacidad de los sistemas para intercambiar y usar información es una condición fundamental para permitir la soberanía de los datos.	• Tamaño de muestra pequeño de 18 participantes. • Sesgo debido a que los participantes provenían en su mayoría de la investigación en lugar de la industria. • Posible sesgo profesional basado en las áreas de especialización de los participantes. • Sesgo geográfico ya que todos los participantes eran de Europa occidental. • Posible sesgo debido a la preselección de las características del sistema.	La soberanía de los datos no se logra implementando una lista definida de características del sistema, sino mediante una combinación de requisitos funcionales y no funcionales específicos de cada caso de uso.

Nro.	Título	Enfoque Principal	Metodología	Hallazgo Principales	Limitaciones	Contribución a la soberanía de datos
					• Posible sesgo debido al orden de las preguntas	

De acuerdo con los aportes de los expertos en el tema, podemos clasificar los enfoques teóricos en tres dimensiones:

- ✓ Dominio Sociotécnico: técnico, social, ético y de derechos humanos.
- ✓ Dominio Legal: legal, político y de gobernanza de datos.
- ✓ Dominio económico: económico.

Cada una de estas dimensiones ofrece un marco para entender las complejidades de integrar la soberanía de datos a las *entidades gubernamentales, empresas e individuos*. A medida que profundizamos en cada dimensión, se hace evidente que la interconexión entre ellas es fundamental para abordar los desafíos contemporáneos relacionados con la privacidad y la seguridad de la información. Además, es crucial considerar cómo las políticas públicas pueden influir en la implementación de estas dimensiones, promoviendo un enfoque holístico que garantice la protección de los derechos de los ciudadanos mientras se fomenta la innovación y el desarrollo económico.

2.3 Conceptos Claves

2.3.1 Gobernanza de Datos

La gobernanza de datos está apoyada en la soberanía de datos; este genera las políticas, procedimientos y estándares que las organizaciones utilizan para manejar sus datos de manera eficaz, asegurando su calidad, seguridad y cumplimiento con las leyes y regulaciones. La soberanía de datos se preocupa porque los datos estén cumpliendo las leyes y los marcos de gobernanza en el país donde se recopilan, almacenan y procesan.

La gobernanza y la soberanía de datos se relacionan y apoyan de las siguientes maneras:

- **Para el cumplimiento normativo:** Los marcos de gobernanza de datos ayudan a las organizaciones a cumplir con las leyes de soberanía de datos al definir dónde y cómo se deben capturar, almacenar, procesar y transmitir los datos. Un ejemplo, el GDPR de la Unión Europea establece que los datos personales solo pueden salir de la UE si el país receptor proporciona un nivel adecuado de protección [54].

- **Para la localización de datos:** La soberanía de datos a menudo incluye requisitos de localización de datos, que exigen que ciertos tipos de datos se almacenen dentro de las fronteras del país. Una gobernanza de datos eficaz garantiza que las organizaciones cumplan con estas leyes de localización, evitando así repercusiones legales. Por ejemplo, la Ley de Ciberseguridad de China exige que la información personal y los datos importantes recopilados por los operadores de infraestructuras de información críticas se almacenen dentro de China [62].

- **Para la clasificación y gestión:** Los marcos de gobernanza de datos a menudo incluyen mecanismos para clasificar los datos en función de su sensibilidad y los requisitos legales aplicables. Esta clasificación ayuda a identificar qué leyes de soberanía de datos se aplican a conjuntos de datos específicos. [54] propone un marco de gobernanza de soberanía de datos basado en gráficos de conocimiento que ayuda a clasificar los datos e identificar las leyes aplicables pertinentes.

- **Para las transferencias de datos transfronterizas:** La gobernanza de datos también implica la gestión de las transferencias de datos transfronterizas de conformidad con las leyes de soberanía de datos. Es importante porque gestiona los marcos legales en el que se debe mover los datos entre diferentes jurisdicciones y garantizar que las transferencias de estos datos cumplan con los requisitos reglamentarios tanto de los países de origen como de los países que reciben la data. [62] analiza cómo las regulaciones sobre privacidad de datos y transferencias de datos transfronterizas intentan vincular los datos digitales a la soberanía y jurisdicción territoriales.

- **Para la seguridad y privacidad:** Los reglamentos generados por la gobernanza de datos deben garantizar que los datos estén seguros y que se mantenga la privacidad, que son aspectos clave de la soberanía de datos. Las organizaciones deben implementar medidas de seguridad para proteger los datos de accesos no autorizados y violaciones, cumpliendo así con las leyes de soberanía de datos que priorizan la protección de los datos de los ciudadanos [54].

En conclusión, se entiende que la gobernanza de datos apoya a la soberanía dándole la estructura y procesos necesarios para lograr el cumplimiento normativo de las leyes, gestionen los requisitos de localización de datos, clasifiquen los datos de manera adecuada, gestionen las transferencias de datos transfronterizas y garanticen la seguridad y la privacidad de los datos.

2.3.2 Seguridad de Datos

La seguridad de datos es crucial en la soberanía de datos debido a varios factores. La soberanía de datos implica que los datos deben ser gobernados por la jurisdicción del estado o territorio en el que se almacenan y procesan, lo que puede crear vulnerabilidades al almacenar información personal en el extranjero. Las leyes de protección de datos, privacidad y seguridad varían entre países, y el incumplimiento de estas puede resultar en multas significativas y daños a la reputación de las empresas [15].

La seguridad de datos, por otro lado, se centra en proteger la confidencialidad, integridad y disponibilidad de los datos contra amenazas y vulnerabilidades. En el contexto de la soberanía de datos, la seguridad de datos se ve reforzada al cumplir con las leyes de protección de datos locales, que pueden incluir medidas estrictas de seguridad y privacidad [15].

La seguridad de datos es crucial para la soberanía de datos porque garantiza la confidencialidad, integridad y privacidad de la información sensible. En el contexto de la computación en la nube, la seguridad de los datos es esencial para proteger la información valiosa y sensible que se almacena y comparte en servidores de la nube, los cuales pueden no ser confiables y podrían acceder y divulgar la privacidad personal de los usuarios, así como compartir los datos ilegalmente [65].

En resumen, la seguridad de datos es vital para la soberanía de datos porque protege la información sensible de accesos no autorizados y garantiza la privacidad y la integridad de los datos, realizando de esta manera el cumplimiento de las leyes y regulaciones locales, evitando así repercusiones legales y financieras para las organizaciones.

2.3.2 Privacidad de Datos

La privacidad de datos es un requerimiento indispensable para lograr la soberanía de datos, y los principales puntos de convergencia son los siguientes:

Control y Autonomía: La privacidad de datos permite a los individuos ejercer control significativo y efectivo sobre sus datos personales, lo cual es esencial para la soberanía de datos. Sin privacidad, los individuos se convierten en objetos impotentes, incapaces de gobernar sus datos frente a tecnologías avanzadas como la inteligencia artificial y el Big Data [16].

Protección contra la Explotación: La privacidad de datos protege a los individuos contra la explotación por parte de gigantes comerciales y la vigilancia estatal. Sin mecanismos robustos de privacidad, los datos personales pueden ser utilizados sin el consentimiento adecuado, lo que socava la capacidad de los individuos para controlar cómo se recopilan, usan y procesan sus datos [16].

Confidencialidad y Seguridad: La privacidad de datos asegura que la información sensible y valiosa esté protegida contra accesos no autorizados y usos indebidos. En el contexto de la computación en la nube, por ejemplo, la privacidad de datos es fundamental para mantener la confidencialidad de la información compartida y evitar la divulgación de la privacidad personal [65].

Soberanía del Usuario: La gestión descentralizada de las preferencias de privacidad, como se propone en el protocolo de privacidad de datos descentralizado, permite a los usuarios mantener la soberanía sobre sus elecciones de privacidad a través de múltiples servicios digitales. Esto es esencial

para que los usuarios puedan gestionar sus preferencias de privacidad de manera holística y no fragmentada [19].

Empoderamiento del Individuo: La privacidad de datos es un componente clave del empoderamiento del individuo, permitiéndole definir y controlar su identidad tanto en línea como fuera de línea. Esto es fundamental para la autodeterminación digital y la soberanía de datos [16].

En resumen, la privacidad de datos es esencial para la soberanía de datos porque proporciona a los individuos el control, la protección y la capacidad de gestionar sus datos de manera efectiva y segura.

2.3.3 Residencia de Datos

La residencia de datos se refiere a la ubicación geográfica donde se almacenan los datos y es un aspecto crucial para la soberanía de datos. La soberanía de datos implica que los datos están sujetos a las leyes del país en el que se encuentran.

Esto es importante porque diferentes países tienen diferentes regulaciones y leyes sobre cómo se deben manejar y proteger los datos. [32] nos dice “La soberanía de los datos es el concepto de que la información, que ha sido convertida y almacenada en forma digital binaria, está sujeta a las leyes del país en el que se encuentra".

Además, la residencia de datos puede influir en la capacidad de un país para ejercer control sobre sus datos y protegerlos de accesos no autorizados por entidades extranjeras. Esto es particularmente relevante en el contexto de la computación en la nube, donde los datos pueden estar almacenados en servidores ubicados en múltiples países. "Establecer la soberanía de los datos (es decir, controlar y verificar la geolocalización de los datos) es de vital importancia" [32]. En consecuencia, esto ha llevado al desarrollo de marcos y tecnologías para la clasificación de datos, la localización y el cumplimiento de regulaciones en evolución como el RGPD [54].

En resumen, la residencia de datos es fundamental para la soberanía de datos porque determina qué leyes y regulaciones se aplican a los datos y afecta la capacidad de un país para proteger y controlar sus datos.

2.3.4 Computación en la nube

La computación en la nube es importante para la soberanía de los datos porque implica el almacenamiento y procesamiento de datos en diferentes jurisdicciones,

lo que puede generar conflictos en las leyes de protección y divulgación de la privacidad [18].

Las importantes implicaciones geopolíticas asociadas con la computación en nube giran en torno a la nueva capacidad de controlar y aprovechar los datos, que se ha convertido en una fuente crucial de influencia en los ámbitos político, económico, social y estratégico. Este fenómeno ha provocado un aumento notable de la demanda de soberanía digital, lo que ha llevado a numerosos gobiernos a esforzarse por reafirmar la autoridad sobre los datos vitales mediante la implementación de políticas de localización de datos y la reestructuración de los marcos de conectividad enfatiza [26].

Por ejemplo, la Unión Europea adopta una estrategia que combina los mandatos normativos y los instrumentos de política industrial en el marco de la «soberanía de los datos» para salvaguardar la privacidad de los datos en Europa y reducir la dependencia de los proveedores de servicios en la nube estadounidenses. En este contexto, se presentan dos ejemplos destacados, Gaia-X y la Alianza Europea para los Datos Industriales, para ilustrar cómo los principios de soberanía de los datos se están integrando en las iniciativas políticas en curso en la UE. Al vincular la soberanía de los datos con la ausencia de un ecosistema de nube europeo competitivo, se subraya la importancia estratégica de la computación en nube en la UE y se hace hincapié en la necesidad de abordar estas complejidades de manera unificada.

Además, el auge de las plataformas digitales y su control sobre los flujos de datos ha complicado aún más el panorama de la soberanía de los datos. Las plataformas pueden convertirse en activos de vigilancia y herramientas coercitivas, influyendo en los equilibrios de poder geopolítico y planteando preguntas sobre quién establece las reglas en el ciberespacio y quién controla los datos de los usuarios [26].

En resumen, el papel de la computación en la nube en la soberanía de los datos es crucial debido a su impacto en el control jurisdiccional, el poder geopolítico y la regulación de los flujos de datos, lo que requiere estrategias para abordar estos desafíos.

2.3.5 Transferencia de datos

La transferencia de datos, particularmente en el contexto del intercambio de datos, implica el movimiento de datos entre diferentes sistemas, organizaciones o países,

y se rige por varios principios y requisitos para garantizar la seguridad, la privacidad y el cumplimiento de los marcos legales. Un aspecto fundamental de la transferencia de datos es la soberanía de los datos, que se refiere al concepto de que los datos están sujetos a las leyes y estructuras de gobierno del país en el que se recopilan o procesan [9]. El tema de la externalidad de los datos enfatizado por [39] subraya la necesidad imperiosa de que los organismos gubernamentales establezcan regulaciones relacionadas con la gestión de datos o, potencialmente, consideren el concepto de soberanía de datos. Sin embargo, la naturaleza polémica que rodea a la soberanía de los datos tiende a fomentar la discordia entre las naciones, lo que lleva a conflictos entre las naciones, como lo ejemplifican las tensiones entre China y otras entidades globales. Estos conflictos pueden surgir debido a las diferentes interpretaciones sobre la propiedad y el control de los datos y las consiguientes implicaciones en la seguridad nacional y los intereses económicos, por lo que se requieren negociaciones diplomáticas y acuerdos internacionales cuidadosos para mitigar los posibles conflictos. Esto es particularmente importante en los intercambios de datos transfronterizos, donde las diferentes jurisdicciones pueden tener diferentes regulaciones y estándares en materia de protección de datos y privacidad [9]. La falta de consenso sobre el entorno regulatorio adecuado y las barreras a los flujos de datos transfronterizos refleja la necesidad de un nuevo enfoque para gobernar estos flujos. La naturaleza única de los datos y la ineficacia del sistema comercial actual para abordar esta singularidad subrayan la importancia de desarrollar reglas universales e interoperables, tal y como lo indica [1].

Por ejemplo [51] discute cómo la aplicación extraterritorial de la legislación de protección de datos de la UE, como el GDPR, puede ser vista como una forma de extender la soberanía de datos de la UE más allá de sus fronteras. Esta aplicación extraterritorial puede imponer cargas a terceros estados y corporaciones, pero también puede ser justificada por la necesidad de proteger los derechos fundamentales de los ciudadanos de la UE.

Además, las revisiones bibliográficas y las entrevistas realizadas sobre el terreno destacan la importancia de establecer protocolos y acuerdos claros entre las partes involucradas en el intercambio de datos para facilitar una transferencia de datos fluida y segura. Estos protocolos suelen incluir estipulaciones sobre el cifrado de datos, los controles de acceso y los registros de auditoría para supervisar y verificar la integridad y confidencialidad de los datos que se transfieren. Además, los requisitos para el intercambio de datos no son estáticos; evolucionan con los

avances tecnológicos y las amenazas emergentes, por lo que es necesario actualizar continuamente las políticas y prácticas. Las organizaciones deben mantenerse informadas sobre los últimos avances en las tecnologías de transferencia de datos y los cambios normativos para mantener el cumplimiento y proteger la información confidencial [9].

En resumen, el impacto de las transferencias de datos en la soberanía de los datos gira en torno al desafío que enfrentan las naciones para conciliar el imperativo de proteger los datos dentro de sus fronteras con la necesidad de facilitar el intercambio de datos a través de las fronteras nacionales para fomentar las actividades económicas mundiales y los esfuerzos de colaboración.

2.3.6 Localización de datos

La implementación práctica de la soberanía de datos, conocida como localización de datos, puede presentar variaciones en su ejecución y motivaciones influenciadas por factores políticos, culturales y tecnológicos. Este concepto implica la necesidad de que los datos se almacenen y procesen dentro de límites definidos, como indican [9]. La intrincada relación entre la localización de los datos y la soberanía de los datos es notable debido a que la localización de los datos sirve como mecanismo para mantener la soberanía de los datos. Esta práctica garantiza que los datos permanezcan bajo la jurisdicción de un país específico, lo que otorga al país la capacidad de hacer valer su autoridad sobre sus datos y protegerlos contra la interferencia o el acceso externos, tal como describen [9].

Un ejemplo de esto lo podemos observar en China, donde la localización de datos está firmemente establecida bajo el principio de la soberanía de Internet, impulsada por el nacionalismo tecnológico y el concepto de seguridad nacional holística. Según [39], este enfoque estratégico es una combinación de requisitos prácticos de seguridad, ventajas económicas y progreso tecnológico. En China, la soberanía de los datos está influenciada tanto por factores externos como por las capacidades internas del país, y se materializa a través de un sistema impulsado por el gobierno que enfatiza la importancia del almacenamiento local de datos y el escrutinio de los flujos de datos salientes [39].

Si bien la localización de los datos puede reforzar la soberanía de los datos al confinarlos dentro de las fronteras nacionales, el logro de una verdadera soberanía de los datos requiere una comprensión integral de los aspectos técnicos, legales y políticos involucrados. También exige el establecimiento de marcos que faciliten el intercambio autónomo de datos, como destacan [9]. Por ejemplo, la ubicación

geográfica de los datos puede afectar a la eficiencia y la funcionalidad de la computación en nube. Los servicios en la nube suelen basarse en la dispersión de los datos en varios sitios, y la imposición de restricciones a los datos en función de los límites geográficos puede plantear desafíos a estos procesos operativos [61].

En esencia, la localización y la soberanía de los datos son interdependientes en cuanto a su objetivo de ejercer autoridad sobre la información dentro de un territorio específico, ya sea a nivel nacional o comunitario.

Capítulo 3: Análisis de Marcos Legales y Regulatorios

3.1. Legislaciones Internacionales

La soberanía de los datos se refiere a la idea de que la información digital está sujeta a las regulaciones y los marcos gubernamentales del país en el que se recopila o procesa. Esta noción ha recibido una atención significativa como resultado de la creciente naturaleza global de la transmisión de datos y el surgimiento de la computación en nube, una práctica que con frecuencia implica que los datos atraviesen las fronteras internacionales. Las normas que rigen la soberanía de los datos se basan principalmente en las políticas nacionales que estipulan la gestión, el almacenamiento y la protección adecuados de los datos dentro de las fronteras de una nación. Estas regulaciones suelen estar determinadas por preocupaciones relacionadas con la privacidad, la seguridad, la ubicación geográfica, la transferencia y la residencia de los datos; aspectos que anteriormente se identificaron como componentes fundamentales de la soberanía de los datos. Es imperativo reconocer que estas regulaciones son parte integral de los intereses nacionales de cada país.

Actualmente, se han implementado una multitud de legislaciones en todo el mundo (Ver Anexo 1) para garantizar el cumplimiento de los principios fundamentales de la soberanía de los datos. Estas leyes varían en cuanto a su enfoque: algunas hacen hincapié en la seguridad de los datos, otras se centran en la privacidad de los datos y otras se centran en la protección de los datos. Es imperativo clasificar estas leyes geográficamente, normalmente por continentes, para analizar y comprender los países más prominentes y progresistas en este ámbito. Es crucial tener en cuenta la existencia de leyes transnacionales que abarcan varios países, lo que indica un esfuerzo de colaboración para abordar las preocupaciones relacionadas con los datos a una escala más amplia. Como vemos en la Ilustración 3 la mayoría de los países tiene implementada leyes de privacidad de datos en sus leyes.

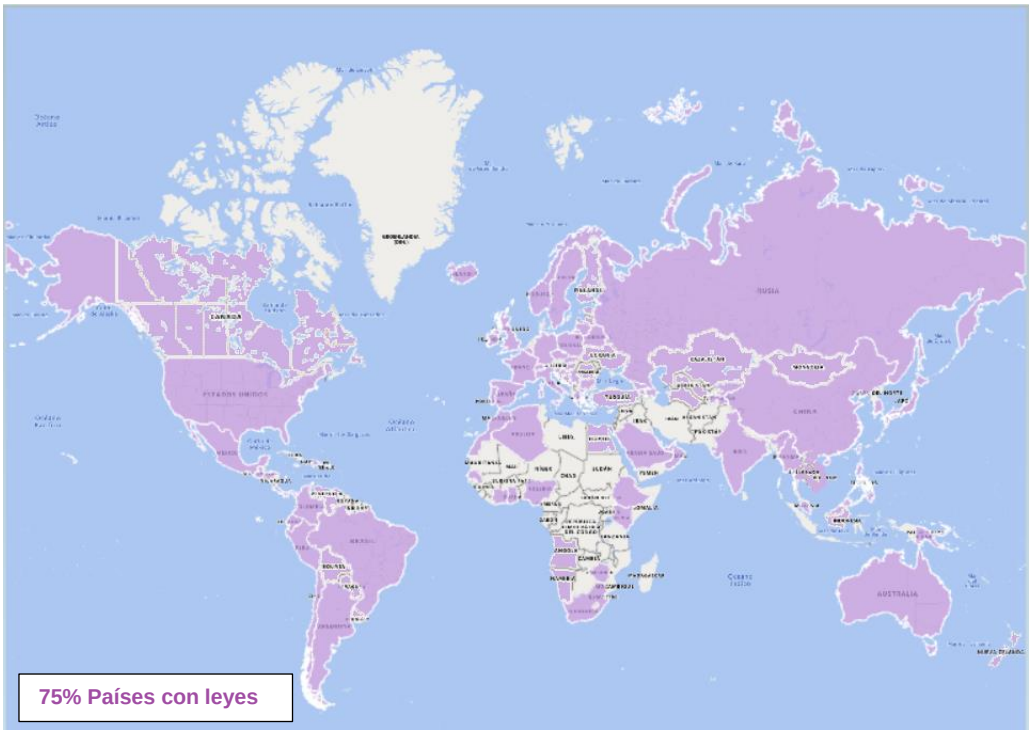

Ilustración 3: Mapamundi de Países con Leyes de Privacidad de Datos

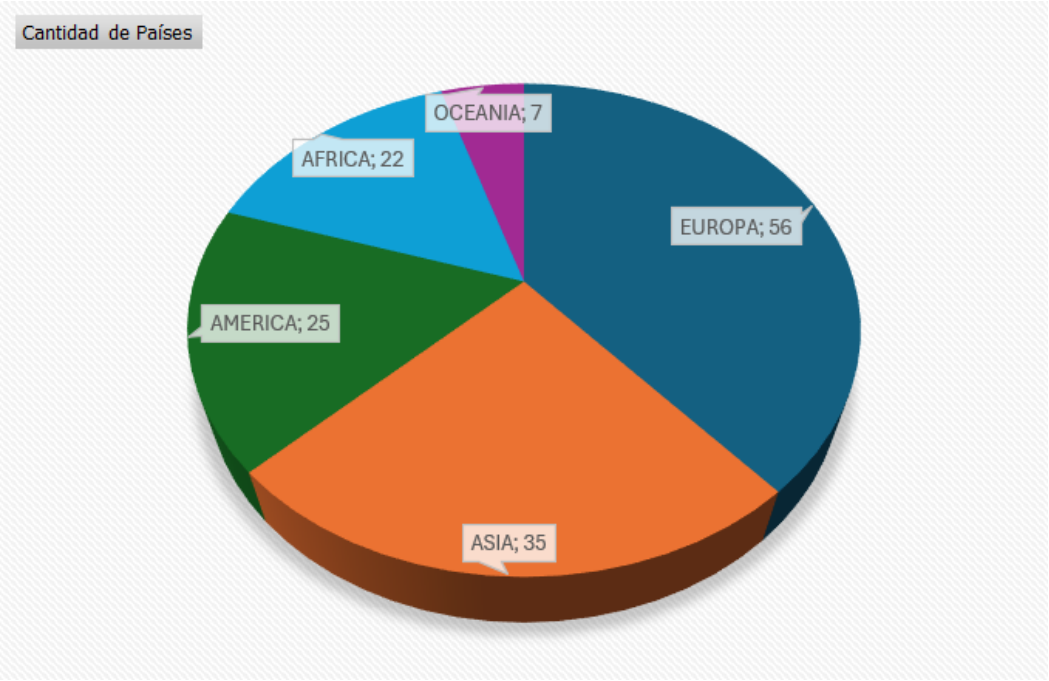

Ilustración 4: cantidad de países por continente con Leyes de Privacidad de Datos

Como se puede visualizar en la Ilustración 4, el Continente Europeo ha tenido un avance significativo en leyes que integren la soberanía de datos. A continuación, daremos detalles por Continente:

- En toda Europa, el Reglamento General de Protección de Datos (GDPR) es la normativa principal que regula la protección de datos, obligando a las empresas y gobiernos a cumplir con estrictos requisitos sobre la privacidad, el almacenamiento y la transferencia de datos. Aunque los países pueden tener normas adicionales o adaptaciones locales, el GDPR garantiza la coherencia en la soberanía de datos dentro de la Unión Europea.
- En América, las leyes de protección de datos varían, pero muchas naciones, especialmente en América Latina, han adoptado leyes similares al GDPR, que restringen la transferencia de datos personales a países que no ofrecen un nivel adecuado de protección. Países como Brasil, Argentina y México tienen leyes robustas de protección de datos, mientras que Estados Unidos carece de una ley federal única, aunque estados como California imponen regulaciones estrictas.
- En Asia, los países están adoptando diversas leyes para proteger la soberanía de los datos personales, con varias naciones implementando regulaciones similares al GDPR de la Unión Europea. China, India y Vietnam han impuesto estrictas leyes de localización de datos, obligando a las empresas a almacenar los datos personales dentro del país, mientras que otros países como Japón y Corea del Sur permiten la transferencia internacional de datos, siempre que se garantice una protección adecuada. Los Emiratos Árabes Unidos y Arabia Saudita también han establecido reglas estrictas sobre la localización de datos, buscando garantizar la soberanía de la información de sus ciudadanos.
- En Oceanía, Australia y Nueva Zelanda son los países más avanzados en términos de regulación de la soberanía de datos, con leyes de Privacidad de datos robustas (Privacy Act 1988 y Privacy Act 2020 respectivamente) y que especialmente limitan la transferencia de datos personales solo a países que ofrezcan un nivel adecuado de protección. Ambos países permiten la transferencia de datos al extranjero bajo acuerdos contractuales que aseguren la protección de la información (ambos pertenecen al Foro de Cooperación Económica Asia-Pacífico que ha implementado el Privacy Framework). Otros países de la región, como Fiyi, Samoa y Vanuatu, han comenzado a implementar leyes para proteger los datos personales y

establecer normas para la transferencia internacional de datos guiándose las normas más utilizadas como la GDPR, aunque no todos los países de Oceanía tienen leyes específicas sobre la localización de datos o soberanía datos.

- En África, varios países han implementado leyes de protección de datos personales, muchas de ellas inspiradas en el GDPR de la Unión Europea, que regula la transferencia de datos personales a países que ofrecen niveles adecuados de protección. Sudáfrica, Nigeria, y Kenia lideran con leyes robustas como la POPIA y el NDPR, las cuales imponen estrictas restricciones para la transferencia internacional de datos, permitiéndola solo bajo ciertas condiciones o cuando se aseguran protecciones adecuadas. Otros países, como Mauricio, Egipto y Ruanda, han seguido implementando regulaciones similares, mientras que naciones como Senegal y Túnez también tienen marcos regulatorios establecidos desde hace tiempo. África está avanzando hacia una mayor soberanía de datos, con leyes cada vez más alineadas con los estándares internacionales de protección de datos.

3.2. Comparaciones de legislaciones

A continuación, muestro un cuadro (ver Tabla 3) con las leyes más representativas y utilizadas como modelos para regular el cumplimiento de la soberanía de datos perteneciente a diferentes países en diferentes continentes; realizando comparativas con respecto a las características más relevantes de cada una; como sus principios fundamentales, autoridades de protección de datos, derechos de los individuos y sanciones.

TABLA 3: MATRIZ DE MARCOS LEGALES Y POLÍTICOS EN EL MUNDO DE SOBERANÍA DE DATOS

Jurisdicciones	Ley	Principios fundamentales	Autoridades de protección de datos	Derechos de los individuos	Sanciones
Estados Unidos	CCPA (The California Consumer Privacy Act) [131].	• Derechos de privacidad para los consumidores. [78]. • Expansión de la responsabilidad por violaciones de datos de los consumidores [78]. • Obligaciones para las empresas que manejan información personal [78].	Autoridades del Estado de California	• Los consumidores tienen el derecho de saber qué información personal se recopila sobre ellos y cómo se utiliza [78]. • Los consumidores pueden solicitar la eliminación de su información personal [78].	• Los consumidores tienen el derecho a no ser discriminados por ejercer sus derechos de privacidad [78]. • El incumplimiento también puede llevar a acciones legales contra las

				• Los consumidores tienen el derecho de optar por no permitir la venta de su información personal [78]. • Los consumidores tienen el derecho a no ser discriminados por ejercer sus derechos de privacidad [78].	organizaciones [78]. • Además de las sanciones legales y regulatorias, las organizaciones pueden sufrir una pérdida de confianza por parte de los clientes [78].
Estados Unidos	Cloud Act (Clarifying Lawful Overseas Use of Data Act) [130].	• Marco para la divulgación de datos almacenados en EE. UU [24]. • Acuerdos bilaterales “países que respeten los derechos y que cumplan con el Estado de derecho” [24].	• Tribunales y jueces. • Autoridades independientes.	• Protección de la privacidad y las libertades civiles [24]. • Revisión judicial por autoridades independientes bajo la ley nacional de la parte emisora [24]. • Derecho a impugnar órdenes por parte del	Pago de montos entre 40.000 y 600.000 euros en dependiendo de las jurisdicciones y también puede aplicarse sanciones administrativas [24].

		• Levantamiento de restricciones bajo la ley EE. UU. sobre las empresas que divulgan datos electrónicos directamente a las autoridades extranjeras en caso de investigaciones de delitos graves [24]. • Compatibilidad con MLATs (Tratado de asistencia legal mutua) [24]. • Protección de derechos de privacidad, las libertades civiles y un Internet abierto. Supervisión judicial bajo la ley nacional de la parte emisora por una autoridad independiente		proveedor si hay un motivo razonable para que el acuerdo no sea invocado [24]. • Procedimiento de minimización de datos personales de los ciudadanos EE. UU. [24]. • Restricciones en la focalización intencional a ciudadanos, residentes permanentes legales o personas en territorio EE. UU. [24].	

		en el proceso relacionado la ejecución de la orden [24].			
Canadá	PIPEDA (The Personal Information Protection and Electronic Documents Act) [79].	• Las organizaciones deben garantizar la protección de los datos personales que administran designando a las personas responsables del cumplimiento de los principios de privacidad [151]. • Las organizaciones deben determinar los objetivos para los que se recopilan los datos personales antes o durante el proceso de recopilación [151]. • El conocimiento y el consentimiento del	Comisionado de Privacidad de Canadá. Cortes Federales	• Derecho a la Información. • Derecho de Acceso de la información personal. • Derecho a la Corrección de la información personal. • Derecho al Consentimiento para la divulgación de su información personal. • Derecho a la transparencia sobre las políticas y prácticas [151].	• Investigaciones y Recomendaciones del Comisionado de Privacidad [151]. • Tanto el comisionado como el demandante pueden solicitar al Tribunal Federal una orden ejecutiva que ordene a la organización rectificar sus prácticas de privacidad o compensar los

		individuo son necesarios para la recopilación, uso o divulgación de información personal, excepto cuando sea inapropiado [151]. • La información personal debe usarse únicamente para el propósito previsto, salvo consentimiento o requisitos legales. La retención de la información personal debe limitarse al tiempo necesario para su uso previsto [151]. • La información personal debe ser tan precisa, completa y actualizada como sea			daños y perjuicios [151]. • Las sentencias judiciales y las evaluaciones de los comisionados pueden afectar negativamente a la percepción pública y la posición en el mercado de las organizaciones que se considera que no cumplen con la PIPEDA [151].

		necesario para los propósitos para los cuales se va a usar. Las organizaciones deben hacer fácilmente comprensibles sus políticas y prácticas relacionadas con la gestión de la información personal [151]. • Las personas tienen derecho a conocer la existencia y el uso de su información personal. También deberían poder verificar y modificar la exactitud de esta información [151]. • Un individuo debe poder cuestionar el			

		cumplimiento de estos principios con la persona o personas responsables del cumplimiento de la organización [151].			
México	LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) [137].	• El tratamiento de datos debe ser conforme a la ley. • El tratamiento de datos personales requiere el consentimiento del titular. • Los titulares deben ser informados sobre el tratamiento de sus datos. • Los datos deben ser exactos, completos y actualizados.	• Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). • Entidades en los ámbitos federal, estatal y municipal, así como los órganos de los Poderes Ejecutivo, Legislativo y	• Derecho a conocer qué datos personales se tienen y cómo se están utilizando. • Derecho a corregir datos personales inexactos o incompletos. • Derecho a solicitar la eliminación de los datos personales cuando ya no sean necesarios para los fines para los que fueron recolectados.	• Se considera una violación no cumplir con las solicitudes de acceso, rectificación, cancelación u oposición al tratamiento de los datos personales. • Se sanciona a quienes recolecten o transfieran datos personales sin el

		• Los datos deben ser exactos, completos y actualizados. • Los datos deben ser utilizados solo para los fines para los que fueron recolectados. • El tratamiento de datos debe ser leal y no engañoso. • Solo se deben recolectar los datos necesarios para el propósito específico. • Los responsables del tratamiento de datos deben garantizar su protección y cumplir con las obligaciones legales [7].	Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad [7].	• Derecho a oponerse al tratamiento de los datos personales por motivos legítimos [7].	consentimiento expreso del titular. • Está prohibida y sancionada la creación de bases de datos que no cumplan con la ley [7].

Brasil	LGPD (The Lei Geral de Proteção de Dados) [129].	• El tratamiento de datos debe realizarse para propósitos legítimos, específicos, explícitos e informados al titular, sin posibilidad de tratamiento posterior de forma incompatible con esas finalidades. • El tratamiento debe ser compatible con las finalidades informadas al titular, en conformidad con el contexto del tratamiento. • Limita el tratamiento al mínimo necesario para la realización de sus finalidades, con datos pertinentes, proporcionales y no excesivos en relación	Autoridade Nacional de Proteção de Dados (ANPD). Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP) [21].	Acceso, Corrección, Anonimización, bloqueo o eliminación, portabilidad, revocación del consentimiento del dato; derecho a la oposición de tratamiento de datos y revisiones de las automatizaciones de los datos personales [21].	• Una advertencia con indicación de plazo para la adopción de medidas correctivas. • Una multa de hasta el 2% del ingreso de la empresa, limitada a R$ 50 millones por infracción. • Una multa diaria, también limitada a R$ 50 millones por infracción. • La publicitación de la infracción una vez que ha sido confirmada, para que el público esté al tanto.

		con las finalidades del tratamiento. • Garantiza a los titulares de los datos la consulta facilitada y gratuita sobre la forma y la duración del tratamiento, así como sobre la integralidad de sus datos personales. • Los datos deben ser claros, exactos, relevantes y actualizados de acuerdo con la necesidad y la finalidad del tratamiento. • Obliga a los responsables del tratamiento a proporcionar información clara y accesible sobre el tratamiento de los datos			• El bloqueo de los datos personales a los que se refiere la infracción hasta su regularización. • La eliminación de los datos personales a los que se refiere la infracción [21].

		personales a los titulares. • Los agentes de tratamiento deben utilizar medidas técnicas y administrativas aptas para proteger los datos personales de eventuales violaciones, incluyendo eventos dolosos y accidentales. • Se deben adoptar medidas necesarias para impedir que ocurran daños en virtud del tratamiento de datos personales. • Prohíbe el tratamiento de datos para fines discriminatorios ilícitos o abusivos.			

		• Los agentes de tratamiento deben no solo cumplir con las normas, sino también tener la capacidad de demostrar su conformidad, conocido como "accountability" [21].			
Unión Europea	GDPR (The General Data Protection Regulation) [75].	Los datos personales deben ser: - "tratados de manera lícita, leal y transparente en relación con el interesado". - "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines".	• Autoridades de Protección de Datos Nacionales. • Comité Europeo de Protección de Datos (EDPB). • Supervisor Europeo de Protección de Datos (SEPD) [31].	• Derecho de acceso a los datos personales. • Derecho de rectificación de los datos personales. • Derecho de supresión (derecho al olvido) de los datos personales. • Derecho a la limitación del tratamiento de los datos personales.	• *Infracciones menos graves*: Pueden resultar en multas administrativas de hasta 10 millones de euros o, en el caso de una empresa, hasta el 2% del volumen de negocios anual global del ejercicio financiero anterior,

		- "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". - "exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan". - "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines		• Derecho a la portabilidad de los datos personales. Derecho de oposición. Derecho a no ser objeto de decisiones automatizadas [31].	lo que sea mayor. Estas infracciones incluyen, entre otras, violaciones relacionadas con el consentimiento de los niños, la protección de datos desde el diseño y por defecto, el mantenimiento de registros y la notificación de brechas de datos. • *Infracciones más graves*: Pueden resultar en multas administrativas de hasta 20 millones de euros o, en el caso de una

		del tratamiento de los datos personales". - "tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas" [31].			empresa, hasta el 4% del volumen de negocios anual global del ejercicio financiero anterior, lo que sea mayor. Estas infracciones incluyen violaciones de los principios básicos del procesamiento de datos, los derechos de los interesados, las transferencias de datos personales a un tercer país o una organización internacional, y el incumplimiento de las órdenes de las

					autoridades de supervisión [31].
Rusia	Ley Federal No. 242-FZ [135].	• Obligación de seguridad de los datos a los operadores. • La localización del dato debe asegurar este dentro de bases de datos dentro de Rusia. • Presencia Virtual del operador en Rusia. • Intervención de autoridades en el procesamiento de los datos personales en otros países a los operadores extranjeros [135].	Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación de la Federación Rusa [135].	Tener almacenados de sus datos personales en base de datos ubicados en el territorio ruso [135].	• Multas Administrativas. • Restricciones operativas. • Bloqueo de servicios digitales [135].
España	LOPDGDD (Ley Orgánica de Protección de Datos Personales y	• Los datos deben ser exactos y actualizados. • Mantener la confidencialidad de los	• Agencia Española de Protección de Datos (AEPD).	Derechos de acceso, de rectificación, supresión (derecho al olvido), oposición, a la	La legislación delinea un marco de sanciones que ofrece una

	Garantía de los Derechos Digitales) [139]	datos personales tratados. • El consentimiento debe proceder de una declaración o de una clara acción afirmativa, excluyendo el consentimiento tácito. • La edad mínima para prestar consentimiento se fija en 14 años, aunque el RGPD permite que los Estados miembros establezcan una edad inferior, siempre que no sea menor de 13 años. • Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.	• Autoridades autonómicas de protección de datos [50].	limitación del tratamiento, a la portabilidad de datos, transparencia e información y testamento digital [50].	considerable discreción, lo que refleja la diferenciación exigida por el Reglamento General de Protección de Datos (GDPR) a la hora de determinar los montos de las sanciones, al tiempo que regula la interrupción de los períodos de prescripción junto con la imposición de sanciones y medidas correctivas [50].

		• Se reconocen y regulan derechos como el acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos [50].			
Japón	APPI (The Act on the Protection of Personal Information) [127].	• La protección de la información personal de los pacientes y la limitación del uso de dicha información a su propósito original. • La ley también establece mecanismos regulatorios y la mejora de la autoridad reguladora. • Uso de información clínica para estudios	Comité de Protección de Información Personal (PPC).	• Protección de su información personal y la limitación del uso de dicha información a su propósito original. • Los individuos tienen el derecho a que su información personal sea utilizada únicamente con su consentimiento, y en casos donde no se pueda obtener el	Sistema de penalización indirecta basado en violaciones de órdenes.

		observacionales bajo ciertas condiciones.		consentimiento directo debido a la falta de información de contacto actualizada, se deben tomar medidas estrictas de privacidad.	
Corea del Sur	PIPA (Ley de Protección de Información Personal) [83].	• Protección de datos personales y derechos de los sujetos de datos. • Prohibición del uso de información personal para fines distintos al propósito original de recolección. • Pseudonimización y anonimización de datos. • Institución especial para la protección de datos personales [52].	Comisión de Protección de Información Personal. [52].	• Derecho a la protección de datos personales. • Derecho a la privacidad. • Derecho a la pseudonimización y anonimización de datos; cualquier uso de estos datos para investigación científica debe ser aprobado por una Junta de Revisión	Multas (investigación y sanción a los controladores y procesadores de datos) [52].

				Institucional (IRB) [52].	
China	PIPL (Ley de Protección de Información Personal) [81].	• Ámbito de aplicación en el territorio de China y también se extiende a actividades específicas realizadas más allá de las fronteras de China si implican el suministro de bienes o servicios a personas que residen en China o la evaluación y valoración de la conducta de personas en China. • Se establece las normas generales y particulares que rigen el tratamiento de los datos personales, formuladas para	Administración del Ciberespacio de China (CAC). Ministerio de Industria y Tecnología de la Información (MIIT). Oficina de Seguridad Pública (PSB). Administración estatal de regulación del mercado (SAMR) [64].	• Las personas tienen derecho a estar informadas sobre el procesamiento de su información personal. • Las personas pueden tomar decisiones con respecto al procesamiento de su información personal. • Las personas tienen derecho a restringir o rechazar el procesamiento de su información personal. • Las personas pueden solicitar el acceso a su información personal y obtener copias de este.	• Multas que pueden ascender hasta 50 millones de yuanes o el 5% de los ingresos anuales del año anterior, lo que sea mayor. • Las autoridades pueden emitir órdenes exigiendo a las organizaciones que rectifiquen sus actividades de procesamiento de datos. • Las autoridades pueden suspender o cancelar las operaciones

		garantizar que la información personal se administre de manera que respete los derechos de los interesados y preserve la integridad y seguridad de los datos. • Para la transferencia de datos saliente debe garantizar que la información personal esté suficientemente protegida incluso cuando se transmite a través de fronteras internacionales. • Derechos a los interesados, incluido el derecho a estar informados, a tomar decisiones, a limitar o		• Las personas tienen derecho a solicitar que se corrija su información personal si es inexacta o está incompleta. • Las personas pueden solicitar la transferencia de su información personal a otro procesador de datos [64].	comerciales de las organizaciones que no cumplan con la ley. • Las personas cuyos derechos hayan sido violados en virtud de la ley pueden interponer recursos legales [64].

		rechazar el procesamiento de su información personal. • La ley impone obligaciones particulares a los procesadores de datos, incluida la obligación de promulgar los protocolos de seguridad necesarios para proteger la información personal. Los procesadores también son responsables de cualquier daño que resulte de sus actividades de procesamiento de datos [64].			

China	DSL (Ley de Seguridad de los Datos) [80].	• La DSL se centra en prevenir los daños a la seguridad nacional y al interés público a través de medios basados en datos. • La DSL tiene como objetivo reorganizar la forma en que se recopilan, almacenan y gestionan los datos en varios actores chinos. • La DSL representa una innovación considerable al abordar problemas de seguridad más amplios. Esto incluye la protección de la infraestructura de datos crítica y la prevención de los riesgos relacionados con los	Organismos de Gobierno y Reguladores de sectores involucrados [17].	El objetivo principal de esta ley es prevenir los daños a través de medios basados en datos, lo que sugiere que los derechos individuales podrían no ser el objetivo central de esta ley [17].	Multas, restricciones comerciales y otras sanciones por incumplimiento [17].

		datos que podrían afectar a la seguridad nacional. • La DSL proporciona un nuevo enfoque de la protección de datos que puede someterse a un análisis comparativo con otros regímenes internacionales de protección de datos [17].			
India	DPDPA (The Digital Personal Data Protection Act) [123].	• Limitar la recolección de datos personales y proporcionar un aviso de privacidad claro y sencillo sobre los propósitos justificados de la recolección de datos. • Prohibir la retención de datos personales más	• Junta de Protección de Datos de India. Es responsable de desarrollar medidas Oficial de Protección de Datos (DPO), asignado por los proveedores de servicio como punto de contacto.	• Derecho a ser informados sobre la recolección y el propósito de sus datos personales a través de un aviso de privacidad claro y sencillo. • Los usuarios deben dar su	• Las penalidades pueden oscilar desde INR 10,000 por incumplimientos menores hasta INR 250 crore (2.5 mil millones de rupias) por infracciones graves relacionadas

		allá del tiempo necesario para cumplir con el propósito para el cual fueron recolectados. • Limitar el procesamiento de datos personales a los fines específicos para los cuales se obtuvo el consentimiento del usuario. • Prohibir la compartición de datos personales sin el consentimiento del usuario y cesar la compartición una vez que se haya cumplido el propósito. • Requerir el consentimiento voluntario del usuario	• Gerente de Consentimiento, individuo registrado en la Junta encargado de gestionar, revisar, otorgar y retirar el consentimiento de los usuarios a través de una plataforma transparente e interoperable [8].	consentimiento voluntario para la recolección y procesamiento de sus datos personales. También tienen el derecho de retirar su consentimiento en cualquier momento. • Derecho de acceder a sus datos personales que han sido recolectados y procesados por los proveedores de servicios. • Derecho de corregir cualquier dato personal inexacto o incompleto.	con la violación de datos personales. • Los proveedores de servicios que no cumplan con las regulaciones pueden ser obligados a proporcionar compensaciones a los usuarios afectados por las violaciones de datos [8].

		para la recolección y procesamiento de datos personales, y permitir la retirada del consentimiento en cualquier momento. • Implementar medidas especiales para proteger los datos personales de los niños. • Otorgar a los usuarios derechos sobre sus datos personales, incluyendo el derecho a acceder, corregir y eliminar sus datos. • Asegurar la implementación de medidas de seguridad adecuadas para proteger los datos personales contra		• Derecho de solicitar la eliminación de sus datos personales una vez que el propósito para el cual fueron recolectados ha sido cumplido. • Derecho a que sus datos personales sean protegidos contra accesos no autorizados y violaciones de datos mediante la implementación de medidas de seguridad adecuadas. • Derecho a ser notificados en caso de una violación de	

		accesos no autorizados y violaciones de datos. • Requerir que los proveedores de servicios informen cualquier violación de datos a la Junta de Protección de Datos de India y a los usuarios afectados. • Exigir que los proveedores de servicios designen un Oficial de Protección de Datos (DPO) para manejar las quejas de los usuarios y asegurar el cumplimiento de las regulaciones. • Establecer penalidades y compensaciones por incumplimiento de las		sus datos personales [8].	

		regulaciones de protección de datos [8].			
Sudáfrica	POPIA (The Protection of Personal Information Act)	• Las organizaciones deben garantizar el cumplimiento de los principios de la ley y son responsables de proteger la información personal. • Regulación del flujo de información personal a través de las fronteras de Sudáfrica. • Hay que asegurar que cualquier limitación al derecho a la privacidad esté justificada y tenga como objetivo proteger otros derechos e intereses importantes.	Regulador de la información; este organismo tiene la tarea de supervisar y hacer cumplir la ley, tramitar las quejas y garantizar que los datos personales se procesen de conformidad con la ley [41].	• Las personas tienen derecho a solicitar el acceso a la información personal que posea una organización. • Las personas pueden solicitar que se corrija su información personal si es inexacta, irrelevante, excesiva, desactualizada, incompleta, engañosa u obtenida de forma ilegal. • Las personas tienen derecho a oponerse al procesamiento de	• Las multas pueden ser importantes, y la sanción máxima puede ser de hasta 10 millones de ZAR, según la gravedad del incumplimiento. • Cargos penales a las personas responsables de la infracción quienes pueden enfrentarse a una pena de prisión de hasta 10 años, según la

		• La información personal debe ser completa, precisa, no engañosa y actualizada cuando sea necesario. • Se debe mantener la documentación de todas las operaciones de procesamiento y hacer que el interesado conozca la información que se recopila y el propósito de esta. • Se debe garantizar la integridad y confidencialidad de la información personal tomando las medidas técnicas y organizativas adecuadas y razonables para evitar la pérdida, el		su información personal en determinadas circunstancias. • Las personas tienen derecho a retirar el consentimiento de tratamiento de su información. • Las personas pueden presentar una queja ante el regulador de la información si creen que su información personal no se maneja de acuerdo con la ley. • Las personas tienen derecho a que se les informe cuando se recopila su	naturaleza del delito. Reclamaciones civiles de las personas afectadas contra las organizaciones por los daños sufridos debido al incumplimiento de la ley [41].

		daño o el acceso no autorizado [41].		información personal y si una persona no autorizada ha accedido a ella [41].	
Nigeria	NDPR (Regulación de Protección de Datos Personales de Nigeria)	• Los datos personales deben ser procesados de manera legal, justa y transparente. • Los datos deben ser recolectados para fines específicos, explícitos y legítimos, y no deben ser procesados de manera incompatible con esos fines. • La recolección de datos debe limitarse a lo que es necesario en relación con los fines para los cuales se procesan. • Los datos personales deben ser precisos y,	Agencia Nacional de Desarrollo de Tecnologías de la Información (NITDA) [38].	• Los individuos tienen derecho a ser informados sobre la recolección y el uso de sus datos personales. • Los individuos pueden solicitar acceso a sus datos personales que están siendo procesados. • Los individuos tienen el derecho de solicitar la corrección de datos personales inexactos o incompletos. También conocido como el "derecho al olvido".	Multas Administrativas y Sanciones Penales. La NITDA puede emitir órdenes de cumplimiento que obliguen a las entidades a tomar medidas correctivas para cumplir con las regulaciones de protección de datos. suspender las operaciones de una entidad hasta que se cumplan los requisitos de

		cuando sea necesario, actualizados. • Los datos personales deben ser precisos y, cuando sea necesario, actualizados. • Los datos deben ser procesados de manera que se garantice una seguridad adecuada, incluida la protección contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental [38].		• Los individuos pueden solicitar la limitación del procesamiento de sus datos personales en determinadas situaciones. • Los individuos pueden obtener y reutilizar sus datos personales para sus propios fines en diferentes servicios. • Los individuos tienen el derecho de oponerse al procesamiento de sus datos personales en ciertas condiciones [38].	protección de datos [38].
Nueva Zelanda	Ley de Privacidad de 2020	• La recopilación de datos personales debe cumplir la función de una agencia legal y ser	Oficina del Comisionado de Privacidad [37].	• Las personas tienen derecho a solicitar el acceso a la información personal	• El Comisionado de Privacidad tiene la autoridad de emitir avisos de

		esencial para ese propósito. • Los datos deben recopilarse principalmente de la persona, a menos que se apliquen excepciones, como la autorización o la disponibilidad pública. • Las agencias están obligadas a informar a las personas sobre el propósito de la recopilación de datos, los destinatarios y sus derechos en relación con la información. • Las agencias deben limitar la recopilación de datos a lo que sea		que posea una organización. • Las personas tienen derecho a solicitar correcciones si es inexacta, incompleta o engañosa. • Las personas tienen derecho a ser informadas sobre el propósito de la recopilación, quién tendrá acceso a ella y sus derechos con respecto a la información. • Las personas pueden oponerse al procesamiento de su información personal en determinadas circunstancias,	cumplimiento a las organizaciones que no se adhieran a la Ley de Privacidad. • Si una organización se niega a proporcionar a una persona el acceso a su información personal, el Comisionado de Privacidad puede emitir una orden de acceso vinculante que obligue a la organización a cumplirla. • La Ley de Privacidad permite imponer sanciones civiles a las organizaciones que

		esencial para los fines previstos. • Los datos personales no deben utilizarse ni compartirse más allá del propósito original sin consentimiento o según lo permita la ley. • Las agencias deben implementar medidas de seguridad adecuadas para proteger la información personal de acciones no autorizadas. • Las personas tienen derecho a acceder a sus datos y solicitar rectificaciones en caso de inexactitudes o datos incompletos.		especialmente si el procesamiento está causando o es probable que cause un daño o angustia sustancial. • En algunos casos, las personas pueden solicitar que se restrinja el procesamiento de su información personal, especialmente si impugnan la exactitud de los datos o si el procesamiento es ilegal. • Si las personas creen que se han violado sus derechos de privacidad, tienen	cometan violaciones graves de la privacidad. Estas sanciones pueden ser importantes y servir como elemento disuasorio contra el incumplimiento. • El Comisionado de Privacidad tiene la facultad de nombrar públicamente a las organizaciones que hayan infringido gravemente las leyes de privacidad. • El Comisionado de Privacidad a menudo busca resolver las quejas mediante la

		• Los datos personales no deben conservarse más tiempo del necesario para su uso legal. • Las agencias deben garantizar el cumplimiento de los principios de protección de la información y establecer procesos para abordar las quejas e infracciones [37].		derecho a presentar una queja ante el Comisionado de Privacidad, que puede investigar y mediar en las disputas [37].	mediación y la negociación, con el objetivo de encontrar una solución mutuamente aceptable sin recurrir a sanciones formales [37].

3.3 Casos prácticos del cumplimiento de la normativa y legislación

3.3.1 Cumplimiento de Localización de datos

Caso en China: TikTok, al ser una empresa con sede en China, está sujeta a la Ley de Seguridad Cibernética de ese país, que obliga a almacenar los datos de los usuarios dentro de China y permite al gobierno acceder a esos datos en situaciones específicas. Esto ha generado preocupaciones sobre la seguridad de los datos de usuarios extranjeros [124].

Caso en Rusia (Ley Federal No. 242-FZ): En Rusia, Amazon y otras empresas tecnológicas deben cumplir con la Ley Federal No. 242-FZ, que exige que los datos de los ciudadanos rusos se almacenen localmente. Esto ha forzado a empresas como Amazon a modificar su infraestructura para operar en Rusia o enfrentar restricciones [102].

Caso en India: Este ha bloqueado el uso de TikTok y otras aplicaciones chinas en su territorio, citando preocupaciones de seguridad y soberanía de datos. El Proyecto de Ley de Protección de Datos Personales de India del 2023 también establece estrictas reglas de localización de datos, exigiendo que los datos personales de los ciudadanos indios se almacenen dentro del país [114].

3.3.2 Protección de datos personales

Caso en la UE (GDPR): En 2019, Google fue multado con 50 millones de euros por la autoridad francesa de protección de datos (CNIL) por violar el GDPR. El incumplimiento se debió a la falta de transparencia en cómo Google gestionaba los datos de los usuarios y la falta de consentimiento explícito para la personalización de anuncios. Según el GDPR, los datos de los ciudadanos de la UE deben gestionarse con un nivel muy alto de protección, y la transferencia de datos a EE. UU. requiere garantías adecuadas, como el uso de Cláusulas Contractuales Estándar (SCC) [141].

Caso en Brasil (LGPD): El Gobierno de Brasil prohíbe a Meta usar datos de usuarios para entrenar modelos de IA. La (Autoridad Nacional de Protección da Datos) ANPD ordenó el cese inmediato de la reciente política de privacidad de Meta implementada a fines de junio del presente año. La ANPD afirma que Meta no proporcionó «información adecuada y suficiente» sobre el novedoso procesamiento de datos personales a los

usuarios, quienes encontraron «obstáculos excesivos e injustificados» para oponerse a esta política [67].

Caso Italia: Multa a Eni Gas e Luce con 11,5 millones de euros por múltiples infracciones del RGPD**,** tuvo una primera multa de 8,5 millones de euros se impuso porque se descubrió que EGL *procesaba ilegalmente datos personales* al realizar llamadas de marketing a personas que habían optado por no recibir dichas llamadas promocionales. La SA italiana también determinó que la empresa no siguió los procedimientos específicos que le exigían verificar el registro público de personas que habían optado por no recibir dichas llamadas promocionales.

La segunda multa que ascendió a 3 millones de euros sancionó a EGL por la celebración de contratos no solicitados (o, básicamente, la inclusión de nuevos clientes en los contratos de EGL sin informarles de que EGL era ahora su compañía energética) y por el uso de información inexacta y, en ocasiones, falsificada en dichos contratos [112].

3.3.3 Cumplimiento de la Privacidad de datos

Caso Nigeriano: El gobierno nigeriano impuso una multa a Meta Platforms por el manejo inadecuado de los datos personales. Las autoridades también señalaron casos de prácticas discriminatorias.

Meta Platforms está obligada a pagar 220 millones de dólares tras las conclusiones de la Comisión Federal de Competencia y Protección del Consumidor (FCCPC) de Nigeria sobre infracciones de la normativa local en materia de datos.

La FCCPC sostuvo que Meta utilizó ilegalmente los datos de los usuarios nigerianos, explotó su poder de mercado con políticas de privacidad perjudiciales y mostró un trato discriminatorio hacia los usuarios nigerianos en comparación con otras regiones (FRANCE24, 2024).

Caso UK: La Oficina del Comisionado de Información del Reino Unido emitió una sentencia contundente contra una empresa por *compartir datos ilegalmente*. La empresa vendió 34,4 millones de registros de usuarios a empresas externas como Equifax (la famosa por sus violaciones de datos) sin informar a los titulares de los datos. Los datos incluían incluso la fecha de nacimiento y el sexo de los recién nacidos. La ICO multó a la empresa con 400.000 libras esterlinas [112].

3.3.4 Restricciones en la transferencia de datos

Caso UE: En julio de 2020, el Tribunal de Justicia de la Unión Europea (TJUE) invalidó el Privacy Shield, un acuerdo que *permitía la transferencia de datos personales* de la UE a EE. UU., argumentando que las leyes de vigilancia estadounidenses no proporcionaban suficientes protecciones a los datos de los ciudadanos europeos. Este fallo, conocido como Schrems II, obligó a las empresas a buscar nuevos mecanismos, como las Cláusulas Contractuales Estándar (SCC), para la transferencia legal de datos fuera de la UE [89].

ILUSTRACIÓN 5: LOS PRINCIPALES ASPECTOS CONSIDERADOS PARA EL CUMPLIMIENTO DE LA SOBERANÍA DE DATOS

Como podemos ver en la Ilustración 5, encontramos cuatro aspectos principales que son base de las legislaciones para el cumplimiento de la Soberanía de Datos.

3.4 Tendencias Globales

Las tendencias mundiales en las leyes que cumplen con la soberanía de los datos reflejan una compleja interacción de los intereses nacionales, la dinámica del comercio internacional y los avances tecnológicos en evolución, estas son:

- Una tendencia importante es el creciente ***énfasis en la localización de los datos***, donde los países exigen que los datos sobre sus ciudadanos o residentes se

recopilen, procesen y almacenen dentro de sus fronteras. Esto se considera una forma de proteger la seguridad nacional y garantizar la privacidad de los datos.

- En la actualidad, los mandatos relativos a la soberanía de los datos se han promulgado en 113 países, principalmente en relación con la ***protección y la confidencialidad de la información personal con un 59 % de países priorizan esta característica,*** la transferencia de datos con un 32%, la privacidad de datos un 34%, los derechos de los individuos 21%, transparencia y rendición de cuentas 17%, localización de datos 15% y seguridad de datos 14%; todo ello con el objetivo de proteger la información nacional confidencial de las amenazas externas.
- El ***GDPR sirve como referencia fundamental para el establecimiento de estas regulaciones***, complementado por directivas de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) [96]. El GDPR de la UE establece normas estrictas sobre el procesamiento y la transferencia de datos, haciendo hincapié en la protección de los datos personales y la privacidad [30].
- A nivel mundial, ***existe una divergencia en la forma en que las diferentes regiones abordan la soberanía de los datos***. Los Estados Unidos, China y la UE defienden diferentes aspectos de la soberanía (empresarial, estatal e individual, respectivamente), lo que da lugar a marcos legales variados y a posibles conflictos en los acuerdos comerciales internacionales [25]. Esta divergencia se complica aún más por las tensiones geopolíticas, ya que los países se esfuerzan por afirmar el control sobre los espacios digitales y proteger los datos de sus ciudadanos de la influencia extranjera [14].
- El concepto de soberanía digital también se está explorando en el ***contexto de la descolonización y los derechos indígenas***. La investigación destaca el impacto del neocolonialismo digital en el Sur Global y aboga por marcos legales que protejan las culturas y los derechos indígenas. Esto incluye abordar las cuestiones del acceso a los datos, la privacidad y la protección de los ecosistemas ambientales, orientando así la legislación mundial sobre datos hacia una gobernanza más equitativa [48].
- A pesar de estos esfuerzos, el camino hacia una ley de datos global unificada sigue plagado de desafíos. Las conferencias y debates, como los celebrados en Accra y Múnich, revelan tanto la ***convergencia como la divergencia en las leyes de protección de datos de todo el mundo***. Si bien existe un impulso hacia la armonización de las leyes de datos para facilitar los flujos internacionales de datos, los regímenes legales contrapuestos y las reivindicaciones geopolíticas en materia de soberanía digital siguen planteando importantes obstáculos [56].

En conclusión, las tendencias mundiales en materia de leyes de soberanía de datos se caracterizan por la tendencia a lograr un mayor control nacional sobre los datos, impulsada por la preocupación por la privacidad, la seguridad y los intereses económicos. Sin embargo, la diversidad de enfoques legales y el panorama geopolítico complican los esfuerzos por establecer un marco global cohesivo. A medida que las naciones sigan enfrentándose a estos desafíos, es probable que el desarrollo de las leyes de soberanía de datos siga siendo un campo dinámico y en evolución, que requiera un diálogo y una cooperación continuos entre las partes interesadas internacionales.

3.5 Evaluación de la efectividad

La efectividad de las leyes existentes en la protección de la soberanía de los datos varía considerablemente según la jurisdicción, y es un tema complejo con múltiples dimensiones. En la UE, la efectividad es alta debido a regulaciones como el GDPR, que no solo protege los datos dentro de la UE, sino que también extiende su influencia a nivel global, obligando a empresas de fuera de la UE a cumplir con sus estrictos estándares si procesan datos de ciudadanos europeos. Esto ha consolidado la soberanía de los datos en la UE y ha reforzado su posición como un regulador digital global.

En contraste, en países como China y Rusia, las leyes son efectivas en cuanto a la consolidación del control estatal sobre los datos, pero su efectividad está acompañada de costos significativos, como la restricción de libertades individuales y el aislamiento del internet global. La Ley de Ciberseguridad de China, por ejemplo, exige que los datos generados dentro del país se almacenen localmente, lo que fortalece la soberanía de los datos, pero limita la cooperación internacional y plantea preocupaciones sobre la privacidad. De manera similar, la estrategia de Rusia con su "Runet soberano" busca un control casi total del tráfico de internet en su territorio, lo que, si bien es efectivo en términos de control estatal, podría fragmentar el internet y reducir la efectividad en términos de cooperación y protección de datos a nivel global.

Para tener una evaluación de la efectividad que sea medible, es fundamental establecer indicadores claros y específicos que permitan analizar los resultados obtenidos. Como este no es el objetivo de la investigación, se sugiere los siguientes indicadores y métricas, basándome en las comparativas y revisiones de las legislaciones en los diferentes países:

- ***Índice de Cumplimiento Regulatorio:*** Este indicador mide el porcentaje de empresas que cumplen con las regulaciones de soberanía de datos en un país. Un mayor porcentaje indicaría una mayor efectividad de las leyes.
- ***Frecuencia y Severidad de Sanciones:*** El número y la severidad de las sanciones impuestas por el incumplimiento de las leyes de soberanía de datos pueden ser un indicador de la efectividad de estas leyes. Un mayor número de sanciones severas podría indicar un mayor nivel de cumplimiento y, por lo tanto, una mayor efectividad.
- ***Tasa de Incidentes de Seguridad de Datos:*** Un descenso en la tasa de violaciones de datos o incidentes de seguridad en un país podría sugerir que las leyes de soberanía de datos son efectivas.
- ***Inversiones en Infraestructura de Datos:*** La cantidad de inversión en infraestructura local de datos (como centros de datos) podría reflejar el éxito de las leyes de localización de datos, un componente clave de la soberanía de datos.

Capítulo 4: Implicaciones en la Seguridad y Privacidad de Datos

4.1 Análisis de Casos reales

4.1.1 Implicaciones para los Gobiernos

Los clasificamos en función de los temas más destacados y ampliamente investigados:

- ***Control y Protección de Datos Sensibles;*** la soberanía de los datos permite a los gobiernos regular la información generada a nivel nacional, salvaguardando los datos confidenciales pertinentes para la seguridad nacional y la privacidad de los ciudadanos del acceso transnacional no autorizado y, al mismo tiempo, mitigando los riesgos de espionaje y amenazas cibernéticas mediante el almacenamiento y el procesamiento de datos locales, como en el caso de China con su Ley de Ciberseguridad que es el más exigente a nivel mundial, otros casos menos radicales como la Ley de Asistencia y Acceso de Australia, que permite a las autoridades gubernamentales obligar a las empresas de tecnología a proporcionar acceso a información cifrada con arreglo a criterios específicos.
- ***Cumplimiento de Regulaciones y Normativas Locales;*** la soberanía de los datos exige el cumplimiento de las leyes de privacidad locales, como el GDPR, que protege la información personal de los ciudadanos, y los gobiernos están facultados para penalizar a las entidades que no cumplan con las normas; además, permite el establecimiento de normas de protección de datos y estándares de ciberseguridad específicos para cada jurisdicción, esenciales para salvaguardar la infraestructura crítica.
- ***Limitación del Flujo Transfronterizo de Datos;*** los gobiernos pueden limitar las transferencias de datos para protegerse contra la explotación en jurisdicciones con estándares de privacidad y seguridad inferiores, que abarcan información crucial como los datos financieros y de telecomunicaciones, que pueden influir en las relaciones comerciales y diplomáticas, aunque estas medidas se consideran esenciales para proteger los intereses nacionales. En el caso de la Ley Federal No. 242-FZ de Rusia que limita el flujo de datos al exigir que todos los datos en internet pasen por servidores ubicados en el país, lo que incluye la capacidad de aislar el internet ruso del resto del mundo si lo considera necesario.
- ***Ciberseguridad Nacional;*** La soberanía de los datos mejora la ciberseguridad al permitir a los gobiernos formular estrategias de seguridad personalizadas para abordar las amenazas localizadas, lo que fomenta las capacidades nacionales para

la detección de incidentes, la respuesta y la protección contra ciberataques específicos, al tiempo que garantiza que los datos de la infraestructura crítica permanezcan protegidos a nivel nacional contra interrupciones externas como el ransomware o el sabotaje. Un ejemplo de ello es la LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales), que sirve como marco legislativo que rige los asuntos de ciberseguridad en España.

- ***Impacto Económico y Tecnológico;*** Al exigir el almacenamiento y el procesamiento de datos locales, los gobiernos pueden fomentar el crecimiento de las infraestructuras tecnológicas nacionales, mejorar las economías locales e impulsar la innovación en el sector tecnológico, aunque estas políticas de soberanía de datos pueden imponer desafíos operativos y legales a las empresas multinacionales y, al mismo tiempo, promover el desarrollo de soluciones de gestión de datos más resilientes. La Unión Europea, los Estados Unidos y China representan a los principales inversores en infraestructura y avances tecnológicos destinados a fomentar y respetar la soberanía de los datos.
- ***Implicaciones Geopolíticas;*** En una era en la que la información constituye poder, la soberanía de los datos permite a los gobiernos regular la información esencial en medio de conflictos o tensiones geopolíticas, lo que puede restringir el acceso externo durante las sanciones o disputas, lo que fomenta tanto los esfuerzos de colaboración para crear estándares globales de protección de datos como las actividades competitivas por el dominio tecnológico y el control de la infraestructura de datos. Uno de los ejemplos es la polémica ley CLOUD Act de Estados Unidos que en el tema con respecto a lo geopolítico ha generado un intenso debate sobre la soberanía de los datos y el acceso a la información por parte de gobiernos extranjeros.

4.1.2 Implicaciones para las empresas

Los clasificamos según los temas más significativos y examinados a fondo:

- ***Cumplimiento Normativo;*** las organizaciones deben cumplir con los mandatos de soberanía de los datos en cada jurisdicción en la que operan, lo que exige el almacenamiento y el procesamiento locales de los datos o el cumplimiento de las estrictas estipulaciones de transferencia de datos. El incumplimiento puede conllevar sanciones importantes y dañar su reputación, especialmente para las empresas multinacionales que se rigen por diversas normativas, como el RGPD en Europa, la LGPD en Brasil y la Ley de Protección de Datos Personales en la India, lo que puede requerir una segmentación regional de los datos y ajustes localizados en la política de privacidad y seguridad.

- ***Seguridad de la Información;*** la soberanía de los datos mejora la seguridad al exigir la gobernanza local del almacenamiento y el procesamiento de los datos, mitigando así la exposición a las ciberamenazas en las jurisdicciones menos seguras; sin embargo, la fragmentación resultante en «islas de datos» puede ampliar la superficie de ataque y complicar la gestión general de la seguridad de la información. Empresas como Microsoft ofrecen el cumplimiento de las normas y regulaciones nacionales & internacionales como el RGPD o el CCPA en sus servicios como Microsoft Azure y otros [134].
- ***Control y Gobernanza de Datos;*** las organizaciones deben intensificar la supervisión de las ubicaciones de almacenamiento y procesamiento de datos, lo que podría adoptar tecnologías sofisticadas de cifrado y administración de claves, al tiempo que implementan políticas sólidas de gobierno de datos que abarquen la clasificación de datos, el control de acceso y las auditorías de cumplimiento para cumplir con las regulaciones de soberanía de datos. Otra de las grandes empresas tecnológicas como Google señala explícitamente como parte de sus políticas en cumplimiento de los Requisitos europeos que el “responsables del tratamiento de datos depende del lugar en el que te encuentres” [117].
- ***Costos Operativos;*** el cumplimiento de los mandatos de soberanía de los datos puede aumentar considerablemente los gastos operativos, lo que requiere inversiones en infraestructuras localizadas, como centros de datos regionales o servicios de nube especializados, y, a menudo, requiere la replicación de la infraestructura en varias jurisdicciones, lo que aumenta los costos de mantenimiento, soporte y administración, además de aumentar la complejidad y los gastos de TI mediante la implementación de soluciones personalizadas para cada región. La empresa mundial Uber describe en su página web sobre Aviso de privacidad describe las prácticas que ha implementado de acuerdo con las leyes de cada país; en especial en Nigeria en donde se procesa los datos de sus usuarios en el país, lo que llevo a invertir en infraestructura tecnológica [99].
- ***Impacto en la Innovación;*** las regulaciones de soberanía de datos pueden obstaculizar la innovación corporativa en tecnologías globales que dependen de los datos, como la IA y los macrodatos, al segmentar el acceso a los datos, pero al mismo tiempo pueden fomentar los avances tecnológicos locales que se alinean con el cumplimiento normativo, creando así oportunidades específicas para el mercado. Uno de los incidentes más sonados de este año involucró a META, que se vio obligada a detener sus avances en Inteligencia Artificial en la Unión Europea y Brasil debido a las deficiencias en la transparencia con respecto a la utilización de los datos de sus ciudadanos. Meta ha expresado su descontento con estas determinaciones,

argumentando que constituyen un importante obstáculo para la innovación y pospondrán las ventajas de la IA para sus usuarios [128].

- ***Relaciones con Proveedores y Terceros;*** las empresas deben garantizar el cumplimiento de las normas de soberanía de datos entre los proveedores y socios, lo que podría requerir más auditorías y renegociaciones de contratos para garantizar una gestión adecuada de los datos dentro de la cadena de suministro; quienes transfieran datos entre jurisdicciones deben adoptar medidas de privacidad y seguridad mejoradas, como cláusulas contractuales estándar y acuerdos de transferencia de datos, junto con medidas de protección adicionales durante el intercambio de datos. Amazon Web Services (AWS) estableció asociaciones con empresas chinas como Sinnet, lo que le permitió continuar operando en el mercado chino cumpliendo con la normativa local. Esta asociación significaba que los servicios de AWS en China estarían bajo el control y la propiedad de una empresa local, cumpliendo así con la ley [150].
- ***Riesgos de Cumplimiento y Litigación;*** el incumplimiento de las leyes de soberanía de datos puede conllevar importantes repercusiones financieras, limitaciones operativas y problemas de litigación, como lo demuestra la imposición por parte del RGPD de multas de hasta el 4% de los ingresos anuales mundiales por infracciones graves de la privacidad, además de posibles disputas legales en varias jurisdicciones que aumentan las complejidades operativas y aumentan el riesgo de costosas y prolongadas confrontaciones legales.
- ***Reputación Corporativa****;* el cumplimiento de las leyes de soberanía de datos mejora la reputación de una organización al demostrar su dedicación a la seguridad y la privacidad de los datos, lo que fomenta la confianza de los clientes en los mercados sensibles a la privacidad, mientras que el incumplimiento puede socavar gravemente la reputación, erosionar la confianza y disminuir el valor de la marca. TikTok, propiedad de la empresa china ByteDance, enfrentó un intenso escrutinio en EE. UU. sobre cómo manejaba los datos de los usuarios estadounidenses. Las preocupaciones sobre la soberanía de datos llevaron a que el gobierno de EE. UU. exigiera que TikTok separara su operación estadounidense de la empresa matriz china.

4.1.3 Implicaciones para los individuos

Los clasificamos según los temas más importantes y examinados minuciosamente.

- **Mayor Control sobre los Datos Personales;** la soberanía de los datos mejora los derechos de privacidad individuales al otorgar un mayor control sobre los datos personales a través de regulaciones locales como el GDPR, que permite a las

personas acceder, corregir y eliminar sus datos, minimizando así la explotación no autorizada.

- **Protección contra Acceso Externo;** la soberanía de los datos se refiere al requisito de que los datos personales se almacenen y procesen dentro de las fronteras de una nación, de conformidad con su marco legal, lo que protege a las personas del acceso no autorizado por parte de entidades extranjeras y mitiga el riesgo de espionaje, especialmente para quienes administran información confidencial en regiones propensas a la vigilancia. En 2013, Edward Snowden dio a conocer los programas de vigilancia masiva de la Agencia de Seguridad Nacional (NSA), incluido PRISM, que acumulaba una gran cantidad de datos sobre personas. La recopilación de datos de servidores extranjeros por parte de la NSA puso de relieve las complejidades de la soberanía de los datos en el acceso internacional a la información [113].
- **Desafíos en la Portabilidad y Acceso Global a los Servicios;** la soberanía de los datos puede obstaculizar el acceso de las personas a los servicios extranjeros debido a las restrictivas regulaciones de transferencia de datos, lo que complica la portabilidad de los datos personales para los usuarios que navegan entre jurisdicciones o utilizan aplicaciones globales. Este ejemplo lo podemos encontrar en el Artículo 20 considerando 68 del RGPD y en las Directrices del CEPD sobre la portabilidad de datos [104].
- **Protección contra la Explotación de Datos;** la soberanía de los datos protege a las personas de la explotación comercial de los datos personales al imponer regulaciones locales que requieren el consentimiento explícito del usuario y exigen la transparencia en relación con el uso de los datos, lo que mitiga el riesgo de uso indebido, en particular por parte de empresas de jurisdicciones con estándares de privacidad laxos. La controversia de Cambridge Analytic que surgió en 2018 se refería a la adquisición y explotación no autorizadas de la información personal de innumerables usuarios de Facebook, ejecutadas sin su permiso explícito. Esta información se empleó estratégicamente para influir en los resultados políticos, en particular en las elecciones presidenciales de Estados Unidos de 2016 [72].
- ***Seguridad y Resiliencia en la Protección de Datos;*** la soberanía de los datos facilita el almacenamiento y el procesamiento de datos localizados, lo que permite a los gobiernos aplicar estrictas normas de ciberseguridad que protegen la información personal de las ciberamenazas, ofreciendo así una mayor protección contra las deficiencias de los sistemas internacionales que carecen de protocolos de seguridad equivalentes. Estonia utiliza tecnologías avanzadas de criptografía, blockchain, y autenticación digital para asegurar que los datos personales de sus ciudadanos

estén protegidos. Cada ciudadano tiene una ID digital que permite el acceso seguro a todos los servicios en línea, y se implementa el KSI blockchain para asegurar la integridad de los datos y prevenir el acceso no autorizado [97].

- ***Confianza en el Manejo de Datos;*** la soberanía de los datos mejora la confianza de las personas en las instituciones que manejan datos al garantizar la protección legal local de sus datos, fomentando así la confianza en las empresas que se adhieren a dichas regulaciones y aumentando la propensión a compartir información personal. Gaia-X se basa en principios de soberanía de datos, asegurando que las empresas y usuarios europeos tengan control sobre sus datos. Utiliza estándares abiertos, interoperabilidad y cumplimiento con la Regulación General de Protección de Datos (GDPR) para garantizar la privacidad y seguridad en toda la infraestructura [108].
- ***Implicaciones en la Libertad de Expresión y Derechos Digitales;*** en algunos países, la soberanía de los datos puede servir como mecanismo para censurar la información o limitar el acceso, ya que los gobiernos pueden exigir el almacenamiento local de datos en las plataformas en línea, lo que mejora la vigilancia y el control sobre el intercambio o la accesibilidad de la información individual; si bien la soberanía de los datos puede mejorar la seguridad y la privacidad, también puede manipularse para intensificar la supervisión gubernamental de los ciudadanos, particularmente en los regímenes autoritarios. Como en los países de China, Rusia, Estados Unidos con legislaciones que intentan censurar información o limitar accesos para usos políticos o gobiernos autoritarios.
- ***Incertidumbre en el Acceso a Justicia y Recursos;*** la soberanía de los datos denota que los conflictos relacionados con la utilización de los datos personales se resuelven según el marco legal del país que aloja los datos, lo que puede exponer a las personas a protecciones legales desconocidas o insuficientes, especialmente cuando sus datos abarcan varias jurisdicciones, lo que complica la identificación de las leyes aplicables y las vías de recurso legal en casos de compromiso o mala administración de los datos. Max Schrems, un activista de privacidad austriaco presentó demandas contra Facebook en relación con la transferencia de datos personales de la UE a EE. UU. Estas demandas llevaron a la invalidez del acuerdo de Safe Harbor en 2015 y más tarde del Privacy Shield en 2020 por el Tribunal de Justicia de la Unión Europea (TJUE).

Ilustración 6: Implicaciones de la Seguridad y Privacidad de Datos

Como se muestra en la ilustración 6, se han consolidado los principales aspectos en los que la seguridad y la privacidad de los datos ejercen influencia; esta representación gráfica resume el discurso antes mencionado.

4.2. Cifras y Estadísticas

Esta sección describe las estadísticas y los datos empíricos importantes relacionados con la implementación y la utilización de los estatutos legales y los marcos regulatorios empleados para cumplir con la soberanía de los datos en varias jurisdicciones, junto con sus implicaciones para la protección de la privacidad y la seguridad de la información.

ESPAÑA

La Agencia Española de Protección de Datos (AEPD), en su Memoria Anual 2023 nos da las siguientes cifras [90]:

- ***111,000 delegados*** de protección de datos notificados ante la Agencia, que realizan trabajo preventivo y de colaboración.
- Aumenta un incremento cuantitativo y cualitativo del ***43% en el 2023***, en el volumen de reclamaciones planteadas ante la Agencia de Protección de Datos.
- Durante el año 2023 se ha dictado por la Sala de los contencioso-administrativos de la Audiencia Nacional, ***43 resoluciones*** de la AEPD.
- En total, como consecuencia de las responsabilidades descritas en el artículo 34 del GDPR, los controladores de datos informaron a casi ***17 millones de sujetos de datos afectados*** sobre la ocurrencia de una violación de datos que afectara a su información personal. Se ha recibido ***2.004 notificaciones de estas brechas de datos personales*** según artículo 33 y se han emitido ***30 resoluciones para obligar a comunicar las brechas a interesados***.
- Se ha contestado en 2023 ***más de 50.000 consultas individuales*** de los ciudadanos, escritas, formuladas a través de la sede electrónica, telefónicas y mediante la atención presencial.
- Un total de ***51.544 ciudadanos han recibido formación sobre sus derechos de protección de datos y sus procesos de reclamación***. Además, se han implementado iniciativas para mejorar la comprensión de los riesgos, las garantías y los derechos relacionados con el procesamiento de datos.
- Los resultados del ***Chatbot*** en su primer año de funcionamiento han sido excelentes, arrojando unas cifras de ***17.337 consultas resueltas en 7 meses de***

funcionamiento y con un nivel de satisfacción reportado por los propios usuarios del 75%.

- La AEPD ha analizado la práctica nivel de cumplimiento y la protección de los datos personales de los ciudadanos en más de ***10.000 entidades del sector público y privado***.
- La mayor multa impuesta en el año se corresponde con un procedimiento del sector de las entidades financieras, en el que se impone a Caixabank S.A., por ***infracción*** de los artículos 5.1.f, 25 y 32 del ***RGPD***, una ***multa de 5 millones de euros.***
- En 2023, hubo ***un aumento notable del 114% en las quejas relacionadas*** con publicidad no solicitada en comparación con 2022, lo que constituye el 20% del total de quejas recibidas.
- ***509 entidades*** adheridas al Pacto digital para la protección de personas.

UNIÓN EUROPEA

European Data Protection Supervisor nos muestra las siguientes cifras en su Reporte Anual del 2023 [152]:

- ***77 números de notificaciones de violaciones de datos personales*** ha disminuido en un 19% en comparación del 2022, principalmente fueron casos de violación de integridad.
- Se presentaron ***58 notificaciones en un plazo de 72 horas*****,** mientras que los responsables de tratamiento retrasaron 19 notificaciones por diversos motivos.
- Las ***causas fundamentales*** de las notificaciones de vulneración de datos personales en el 2023 ***fueron en 44 por error humano***, 16 errores técnico, 9 ataques externo (software espía, suplantación de identidad, etc.), 2 accesos no autorizado y 6 desconocidos.
- En ***un 44% de casos se vieron afectados entre 101-500*** personas, el 29% de casos se vieron afectados entre 1-10 personas, en un 12% se vieron afectado entre 51-100 personas y en el ***4% la mayor cantidad más de 1.000 personas***.
- El ***19% de las notificaciones de violación de datos personales*** recibidas este año involucraron categorías especiales de datos. En la mayoría de los casos se trata de datos de salud, mayoritariamente asociados a errores en el envío de facturas médicas, especialmente durante los procesos de reembolso.
- ***El número de consultas y solicitudes de personas*** que ejercen sus derechos de protección de datos recibida por el SEPD en el 2023 aumento a **43**.
- Eurostat publicó un artículo “Como protegieron los usuarios de Internet sus datos en el 2023” y arrojaron los siguientes datos [105]:

- En 2023, solo el ***36% de los usuarios de Internet de la UE leerán las declaraciones de política de privacidad*** antes de proporcionar datos personales.
- Más de la mitad (**54%**) de los ***usuarios de Internet se negó a permitir el uso de sus datos personales*** con fines publicitarios y algo más de la mitad (51%) restringió o denegó el acceso a su ubicación geográfica. Además, el 41% limitó el acceso a su perfil o contenido en sitios de redes sociales o almacenamiento compartido en línea [105].
- En cuanto a la protección de los datos personales que compartieron, solo el ***35% verificó que el sitio web donde proporcionaron sus datos personales*** fuera seguro [105].
- En 2023, la proporción de usuarios de Internet que accedieron a sus datos personales varió según los países de la UE. Los porcentajes más altos se observaron en ***Finlandia y los Países Bajos (ambos con un 93 %),*** seguidos de República Checa (89 %). Por el contrario, los porcentajes más bajos se registraron en Rumania (52%), Letonia (55%) y Eslovenia (57%) [105].

EE.UU. Y REINO UNIDO

La consultora Womble Bond Dickinson elaboró un informe del 2023 en el que examinaba la legislación sobre privacidad de datos y encuestó a 200 personas de empresas ubicadas en ambos países, y arrojó los siguientes hallazgos:

- Aproximadamente el 50% de las organizaciones de EE.UU. y el Reino Unido dicen estar “muy preparadas” para abordar las leyes de privacidad de datos tanto en Estados Unidos como en Europa [86].
- El 55% de los encuestados estadounidenses están preocupados por la aplicación de la legislación sobre privacidad de los datos de geolocalización, mientras que el 50% afirma lo mismo sobre litigios, una proporción significativamente mayor que la de sus homólogos británicos, con un 45% y un 36%, respectivamente [86].
- Solo el 10% de los encuestados del Reino Unido dicen que las regulaciones de privacidad de datos son un impedimento importante para los negocios transfronterizos [86].
- El 50% de los encuestados de la UE y Reino Unido que dicen que comprender los datos que encuentran dentro de su organización es un obstáculo clave, de estos el 45% desea aumentar presupuesto [86].
- casi el 60% de los ejecutivos que operan en EE. UU. consideran un reto el seguimiento del estado de la legislación y las diferencias entre las leyes estatales, aunque solo el 42% ha realizado comparaciones de los marcos legislativos estatales en materia de privacidad [86].

- El 59% de los encuestados en el Reino Unido este más preparado para el cumplimiento del RGPD y/o DPA, en comparación con solo el 44% de los encuestados en sedes de Estados Unidos [86].
- Solo el 10% de los encuestados en el Reino Unido las considera un obstáculo (costos extras) importante, frente al 17% en los EE. UU [86].
- El uso de datos de geolocalización crea problemas similares; el 40% de los encuestados de EE. UU. frente el 32% de los del Reino Unido, dicen estar muy preocupados por leyes de privacidad que incluyen restricciones específicas sobre la recopilación y el uso de dichos datos para fines de marketing dirigidos. Las preocupaciones principales son los futuros litigios y las acciones para hacer cumplir la ley [86].
- El 59% de los encuestados británicos indican que sus organizaciones utilizan actualmente datos biométricos, y el 64% de los estadounidenses afirman lo mismo, lo que supone un aumento de cinco puntos porcentuales con respecto a 2022. Aunque la mayoría utiliza las huellas dactilares para generar estos datos, sobre todo con fines de identificación inicial o autenticación, no son pocos los encuestados en Estados Unidos y Reino Unido que obtienen información biométrica a partir del reconocimiento del iris (28%), las venas de los dedos o las manos (24%), los latidos del corazón (8%) e incluso las ondas cerebrales (5%) [86].

ESTADOS UNIDOS

Según el reporte de la Trade Commission Annual Report Fiscal Year 2023 sobre la Protección de la privacidad y la seguridad de los datos de los estadounidenses, se reportaron 17 casos (Anexo 2) de los cuales la multa más grande fue la impuesta a la empresa de juegos en línea Epic Games Inc. por su juego Fortnite de 520 millones de dólares, la mayoría de los casos son violaciones a las reglas de COPPA [84], el reporte completo puede revisarse en el Anexo 2.

4.3. Evaluación del impacto

Evaluaremos los casos en el que la integración de la soberanía de datos según los temas en común que he encontrado en esta investigación:

4.3.1 Según los Principios Generales de la Protección de datos

La protección de datos para el cumplimiento de la soberanía de datos requiere un enfoque holístico de diseño de sistemas que integre medidas legales, administrativas y técnicas; en el que los sistemas de identificación se sustenten en marcos legales que protejan los datos individuales, la privacidad y los derechos de los usuarios, y numerosos países promulguen una legislación general de protección de datos y

privacidad aplicable no solo a los sistemas de identificación sino también a diversas actividades gubernamentales y del sector privado que implican el procesamiento de datos personales [121]. Estas leyes suelen tener principios generales específicos para la recopilación, almacenamiento y uso de información personal, que incluyen:

Limitación de la finalidad: La adquisición y la utilización de datos personales deben limitarse a objetivos que (1) estén legalmente definidos y, por lo tanto, sean reconocibles por el interesado en el momento de la recopilación; o (2) para los que el interesado haya dado su consentimiento explícito. Un ejemplo de este principio es que la impuesta por la Unión Europea a Google, esta Compañía Tecnológica como otras empresas recopila grandes cantidades de datos personales de sus usuarios, como historiales de navegación, preferencias, ubicación, etc.; pero bajo el RGPD, los ciudadanos europeos tienen el derecho a controlar cómo se usan sus datos. Esto incluye derechos como el derecho al olvido (eliminar sus datos), el derecho de acceso (saber qué datos se recopilan) y el derecho a la portabilidad (mover sus datos a otros servicios), por lo que Google debe de obtener el ***consentimiento explícito*** de los usuarios antes de procesar sus datos. Google solo puede utilizar los datos recopilados para los fines específicos que ha indicado en sus términos. Si alguien no desea que Google use su información para publicidad personalizada, puede desactivar esta opción, limitando así el uso de sus datos [98].

Proporcionalidad y minimización: Los datos recopilados deben alinearse con los objetivos del sistema de identificación para mitigar la recopilación excesiva de datos y las posibles amenazas a la privacidad. Este principio generalmente se articula como la necesidad de recopilar solo los datos «mínimos necesarios», incluidos los metadatos de las transacciones, para lograr el objetivo designado. Un ejemplo son las Aplicaciones de Ride-Sharing (como Uber o Lyft); con la implementación del principio de minimización, las aplicaciones solo recopilan los datos necesarios para prestar el servicio, como la ubicación actual del usuario (para asignar un coche) y el destino (para calcular la tarifa y ruta). Acceder a contactos o calendario ya no es necesario y debe requerir un consentimiento explícito si lo fuera para alguna funcionalidad opcional.

Legalidad: La adquisición y la utilización de datos personales requieren una base legal, como el consentimiento, los requisitos contractuales, el cumplimiento de las obligaciones legales, la protección de los intereses vitales, el interés público y/o los intereses legítimos. Un caso muy conocido es Consentimiento para el Uso de Cookies; ahora, debido a la legislación como la RGPD, los sitios web deben ofrecer la posibilidad de rechazar cookies no esenciales y solo activar las cookies mínimas necesarias para

que el sitio web funcione, como las que son necesarias para gestionar la sesión del usuario.

Equidad y transparencia: La adquisición, agregación y aplicación de datos personales individuales requiere que dichos procesos se lleven a cabo de una manera que no solo sea justa y equitativa, sino que también se caracterice por un alto grado de claridad y apertura, garantizando que todas las partes interesadas involucradas conozcan plenamente los métodos empleados y las implicaciones de la utilización de sus datos. Por ejemplo, en los procesos de selección de personal; las empresas solo deben pedir la información estrictamente necesaria para la evaluación inicial del candidato, como experiencia laboral y educación. Los datos más sensibles, como la información fiscal, solo deben pedirse si el candidato es seleccionado para el empleo.

Exactitud: Para garantizar la integridad de los datos personales, es imperativo que dicha información no solo sea precisa en su representación, sino que también se mantenga actualizada de manera constante, por lo que cualquier discrepancia o inexactitud que pueda surgir se rectifique con un sentido de urgencia y eficiencia que refleje la importancia de mantener registros de datos precisos. En el caso de recopilación de datos por empresas de comercio electrónico; la tienda solo puede recopilar información relacionada con la compra, como el nombre, dirección de envío y detalles de pago. No puede exigir datos adicionales a menos que estén claramente justificados para una funcionalidad específica (por ejemplo, el uso de un servicio de fidelización o promociones).

Limitaciones de almacenamiento: La información personal, incluidos los metadatos de las transacciones, no debe conservarse durante un período que exceda lo esencial para los objetivos para los que se recopiló y procesó originalmente. En cuanto a los metadatos de las transacciones, las personas pueden tener la opción de determinar el tiempo durante el cual se conservan dichos datos. Anteriormente las empresas solían almacenar grabaciones de videovigilancia indefinidamente, sin justificación específica. Ahora que se aplican las normativas las grabaciones de CCTV (Sistemas de Videovigilancia) deben conservarse solo durante un período razonable (por ejemplo, 30 días). Si no hay incidentes que justifiquen su conservación (como un robo o investigación), deben ser eliminadas automáticamente una vez transcurrido ese tiempo. Esto protege la privacidad de los individuos y limita el riesgo de uso indebido.

Tecnologías de mejora de la privacidad: Los requisitos previos para emplear tecnologías que protejan la privacidad (como la tokenización de distintos números de identidad) implican la mitigación o erradicación de la recopilación de datos personales,

la prevención del procesamiento superfluo o no deseado de los datos personales y la mejora del cumplimiento de la legislación de protección de datos. Un ejemplo es un servicio que usamos habitualmente el pago con tarjetas de créditos; cuando el usuario realiza el pago, la plataforma genera un token (un código único) que reemplaza el número real de la tarjeta. Este token es lo que se transmite al comerciante para procesar el pago. El token no puede ser reutilizado fuera de esa transacción y es inútil para los ciberdelincuentes en caso de que sea interceptado. Los datos reales de la tarjeta permanecen protegidos en un entorno seguro.

Responsabilidad: La gestión de los datos personales de conformidad con los principios antes mencionados requiere la supervisión de una entidad supervisora independiente y competente, así como de las propias partes interesadas. En la actualidad, las entidades o agencias gubernamentales responsables de supervisar y ayudar a los ciudadanos a cumplir con los estatutos legales incluyen predominantemente a las autoridades de protección de datos y los oficiales de protección de datos, entre otros; además, numerosas empresas y organizaciones actualmente establecen comités de cumplimiento y auditoría interna.

4.3.2 Según las Garantías de Protección de Datos

Los puntos siguientes delinean garantías específicas de protección de datos en relación con la supervisión institucional, la seguridad de los datos, el intercambio de datos, las transferencias transnacionales de datos y el consentimiento del usuario; de acuerdo con estos puntos se ha podido especificar ejemplos con la información revisada en el Anexo 1.

Supervisión institucional

La eficacia de una autoridad reguladora autónoma que supervise la protección de datos y la privacidad, en particular en lo que respecta a los sistemas de identificación, depende de su independencia estructural, que abarca la composición, los procesos de nombramiento, el poder de supervisión, la asignación de recursos y la autonomía de toma de decisiones, lo que le permite abordar las quejas públicas, mientras que las personas conservan el derecho a interponer recursos legales externos vinculantes y a la intervención judicial, y la autoridad puede obligar a rectificar o destruir los datos obtenidos de forma errónea o ilegal. Los siguientes cumplen con el encargo:

- La Inspección de Protección de Datos de Estonia, fundada en 1999, es una autoridad supervisora, facultada por la Ley de Protección de Datos, la Ley de Información Pública y la Ley de Comunicación Electrónica.

- En Sudáfrica, la Ley de Protección de la Información Personal estableció el Regulador de la Información, un organismo independiente sujeto únicamente a la Constitución y a la ley.
- En Filipinas, la Ley de Privacidad de Datos de 2012 creó la Comisión Nacional de Privacidad, entidad independiente. La Comisión, que depende del Departamento de Tecnología de la Información y las Comunicaciones, está encabezada por un Comisionado de Privacidad que cuenta con la asistencia de dos Comisionados Adjuntos de Privacidad (uno responsable de los Sistemas de Procesamiento de Datos y otro responsable de Políticas y Planificación).
- En el Reino Unido, la Ley de Protección de Datos de 1984 introdujo la figura del Comisionado de Información que es un organismo regulador independiente que busca monitorear, investigar y hacer cumplir toda la legislación aplicable en materia de protección de datos y privacidad en el Reino Unido (incluida Escocia, en cierta medida).
- En Francia, SecNumCloud es una certificación emitida por la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) de Francia, que establece los requisitos de seguridad para servicios en la nube utilizados por el gobierno francés. Esta certificación asegura que las soluciones en la nube cumplan con altos estándares de seguridad y soberanía de datos.

Seguridad de datos

La protección y el manejo legal de la información personal son fundamentales para mitigar los riesgos de ciberataques a los sistemas de identificación digital. Por esto las normativas y leyes generadas para el cumplimiento de la seguridad y privacidad de datos deben alinearse a las siguientes características:

- ✓ Los marcos legales requieren medidas de seguridad de los datos, como el cifrado de los datos personales, la anonimización, la seudonimización, la confidencialidad, la integridad, las capacidades de recuperación de datos después de un incidente y las evaluaciones de seguridad continuas de los sistemas que manejan datos personales.
- ✓ Numerosas normativas mundiales exigen que los responsables del tratamiento informen a los interesados de las infracciones importantes relacionadas con su información personal.
- ✓ Además, los países podrían promulgar leyes destinadas a reconocer y abordar las ciberamenazas, junto con leyes que impongan sanciones por el acceso, la utilización o la modificación ilícitos de los datos.

- ✓ Los marcos legales deben incluir sanciones severas para el acceso, la utilización o la modificación no autorizados de datos personales por parte de los administradores de datos y terceros, incluidas las sanciones por el acceso no autorizado a los sistemas de identificación o bases de datos, el monitoreo o la vigilancia ilícitos, el uso indebido de datos personales, la alteración no autorizada de los datos almacenados y la interferencia con los sistemas de identificación que contienen información personal.

Podemos listar los siguientes ejemplos de leyes que exigen la notificación de violaciones de seguridad:

- El RGPD de la UE exige la notificación inmediata a la autoridad supervisora de cualquier violación de datos personales, idealmente en un plazo de 72 horas, a menos que la infracción represente un riesgo mínimo para los derechos individuales, y exige información detallada sobre la violación, incluidas las categorías afectadas y las posibles consecuencias, al tiempo que exige una notificación oportuna a las personas afectadas cuando se identifique un riesgo alto, que incluya los mismos detalles requeridos.
- La mayoría de los estados de EE. UU. han promulgado leyes de notificación de infracciones que obligan a las entidades a informar a las personas sobre las violaciones de seguridad de la información de identificación personal, y describen las definiciones de las infracciones, los protocolos de notificación y las exenciones aplicables.
- En Sudáfrica, la Ley de Protección de la Información Personal 4 de 2013 exige que el regulador de la información notifique con prontitud a los interesados las violaciones, teniendo en cuenta las necesidades de las fuerzas del orden y las medidas necesarias para restablecer la integridad, al tiempo que garantiza que la notificación prepare a los sujetos para mitigar las posibles consecuencias, incluida la posibilidad de que el regulador dé instrucciones a la parte responsable para que divulgue la información sobre la violación para proteger a las personas afectadas.

Intercambio de datos

A medida que la interconectividad de las bases de datos intensifica los problemas de privacidad, los marcos legales pueden mitigar los riesgos al delinear los propósitos permitidos para el intercambio de datos para las entidades, garantizando que las entidades públicas accedan solo a la información esencial según el principio de «necesidad de saber». Los beneficios del intercambio de datos incluyen una mayor comodidad para las interacciones entre los gobiernos y los ciudadanos, una mejor

prestación de servicios gubernamentales, una transición de servicios simplificada, una mejor gestión de riesgos, un ahorro de costos al eliminar las redundancias y una mayor eficiencia mediante la utilización optimizada de los datos.

El intercambio de información no regulado entre los organismos gubernamentales puede comprometer la privacidad individual y la seguridad de los datos. Por ejemplo, las fuerzas del orden pueden solicitar al personal de identificación que recupere y divulgue datos personales confidenciales. Los casos posteriores de acuerdos de intercambio de datos ilustran la aplicación práctica de este concepto:

- El artículo 4, apartado 2, de la Directiva 2016/680/ UE estipula que los datos personales recopilados para fines alternativos solo pueden procesarse para fines relacionados con la delincuencia si: (a) existe una base legal para tal acción y (b) el procesamiento es esencial y acorde con el propósito original de recopilación de datos.
- En la India, la Ley Aadhaar de 2016 permite la divulgación de información, salvo la «información biométrica básica», previa orden judicial y supeditada a la opinión de la Autoridad de Identificación Única de la India (UIDAI). Además, permite la divulgación de toda la información, incluidos los detalles biométricos básicos, por motivos de seguridad nacional, con sujeción a la autorización del gobierno y a la revisión del Comité de Supervisión.
- En Australia, la Ley Federal de Privacidad de 1988 exige que la información personal recopilada para un propósito específico no pueda reutilizarse sin consentimiento. Se hace una excepción en los casos en que los organismos autorizados consideren «razonablemente necesarios» para la aplicación de la ley. Se requiere la documentación de dicho uso policial para garantizar la rendición de cuentas.

Transferencias transfronterizas de datos

La protección de los datos personales en los intercambios transnacionales ha catalizado un acuerdo global sobre los principios esenciales de protección de datos. Por ejemplo, el Marco de Privacidad de la OCDE postula que los controladores de datos siguen siendo responsables de los datos personales, independientemente de su ubicación geográfica.

Muchos países restringen las transferencias extraterritoriales de datos personales debido a las incertidumbres de la regulación de la protección de datos. Dichas transferencias pueden permitirse si las regulaciones de terceros países se consideran adecuadas. Esto es particularmente importante para los datos personales relacionados con la identificación nacional, el registro civil y el registro de votantes. Los marcos

legales también pueden abarcar acuerdos regionales o internacionales para la interoperabilidad o el reconocimiento mutuo de los sistemas de identificación. Por ejemplo, la RGPD pone los siguientes límites a las transferencias de datos:

- El RGPD de la UE restringe las transferencias de datos personales fuera del EEE (Espacio Económico Europeo), con excepciones. Las transferencias están permitidas si la Comisión Europea comprueba que el país receptor brinda la protección adecuada. Esta determinación requiere una evaluación exhaustiva del sistema nacional de protección de datos, que abarque las salvaguardas de los datos personales y los mecanismos correctivos.
- En julio de 2018, la UE y Japón reconocieron que los sistemas de protección de datos de la otra parte eran equivalentes, lo que llevó a la Comisión Europea a iniciar una decisión de adecuación. Las transferencias a países no pertenecientes a la UE están permitidas en condiciones específicas, como la provisión de «salvaguardias apropiadas» mediante acuerdos legalmente vinculantes, cláusulas contractuales o códigos de conducta aprobados, entre otros métodos [104].

Consentimiento y control del usuario

Un principio fundamental de privacidad afirma que la recopilación de datos personales requiere el consentimiento individual, salvo justificaciones legales alternativas. Para que el consentimiento tenga importancia, las personas deben recibir una información clara sobre la naturaleza y los usos previstos de sus datos. Numerosas normas internacionales y reglamentos nacionales describen excepciones al consentimiento para la recopilación de datos gubernamentales en virtud de la autoridad legal, como en el caso de los sistemas de identificación. Si no se requiere el consentimiento, la transparencia debe seguir ofreciendo explicaciones accesibles para fomentar la confianza pública y mitigar los malentendidos. Se debe informar a los ciudadanos sobre qué información es pública y qué permanece confidencial. Algunas naciones implementan «políticas de privacidad» que articulan, en términos sencillos, los procesos de recopilación y uso de datos personales. Algunos ejemplos de leyes de consentimiento del usuario:

- Al procesar datos personales de categorías especiales, como los datos biométricos, el RGPD de la UE exige el cumplimiento de estipulaciones adicionales, incluida la necesidad de obtener el consentimiento «explícito» de la persona para su procesamiento (artículo 9 del GDPR).
- La Ley de Privacidad del Consumidor de California de 2018 regula ciertas empresas que manejan datos personales de los residentes de California, a partir de 2020. A

diferencia del RGPD, por lo general no exige el consentimiento previo para la recopilación de datos. No obstante, los consumidores deben estar informados sobre los tipos y propósitos de la información personal recopilada en el momento de la recopilación. Se deben incluir más detalles en una política de privacidad en línea o en un sitio web, y es necesario actualizarlos cada 12 meses.

- En Australia, la Ley Federal de Privacidad de 1988 exige que la información personal recopilada para un propósito específico requiera el consentimiento para cualquier otro uso. Existen excepciones para los casos en que los organismos autorizados consideren «razonablemente necesarios» las medidas de aplicación de la ley, incluidas las actividades policiales relacionadas con delitos penales. Se debe mantener la documentación sobre el uso de las fuerzas del orden para garantizar la rendición de cuentas.
- Varios marcos legales, incluidos los de la OCDE, la ONU, el CoE y la APEC, afirman los derechos de las personas a administrar sus datos personales. El «derecho a borrar» puede aplicarse a ciertos datos personales, incluida la información confidencial, como el material genético o los apellidos anteriores. Las medidas legales efectivas deben establecer protocolos claros para que las personas accedan, corrijan y eliminen sus datos personales.

La portabilidad de los datos; permite la transferencia fluida de datos personales a través de los ecosistemas tecnológicos, lo que facilita la diversidad de aplicaciones y reduce la dependencia de los consumidores de proveedores de servicios singulares, al tiempo que mejora la utilidad de los sistemas de identificación y alivia las posibles trampas de los consumidores.

- Un ejemplo de este impacto es en el sector bancario es la implementación de la Directiva PSD2 (Revised Payment Service Directive) en Europa [100], que obliga a los bancos a permitir que los usuarios transfieran sus datos financieros a servicios externos de forma segura. Esto permite a los usuarios compartir su información bancaria con aplicaciones de terceros, como aplicaciones de gestión financiera o plataformas de pago, pero siempre manteniendo el control sobre quién puede acceder a estos datos y para qué fines.

Capítulo 5: Soluciones Tecnológicas para la Soberanía de datos

Tabla 4: Cuadro Comparativo de las Soluciones Tecnológicas que se integran a la soberanía de datos

Solución Tecnológica	Campo de Aplicación	Descripción	Aspecto clave	Ejemplos y referencias
Infraestructura de Nube Soberana Colaborativa	Tecnología de la Información	Servicios de nube diseñados para garantizar que los datos se almacenen y procesen dentro de las fronteras del país, cumpliendo con las regulaciones locales.	Control de datos, localización, cumplimiento normativo.	Espacios de Datos: Gaia-X, IDSA, y Catena-X y otros. Cooperativas de Datos: Cooperativa de Datos de Baviera, Farmerline, y otros. Nubes privadas: Nextcloud, Infomaniak y otros.

Solución Tecnológica	Campo de Aplicación	Descripción	Aspecto clave	Ejemplos y referencias
Geofencing de Datos para el cumplimiento de la soberanía de datos	Redes	Tecnologías que aseguran que los datos no salgan de una ubicación geográfica específica, cumpliendo con las regulaciones de soberanía de datos.	Localización de datos, seguridad, cumplimiento normativo.	MapSafe, Foursquare y otros
Sistemas de Identificación Digital Nacionales	Tecnología de la Información	Soluciones que gestionan y protegen las identidades digitales, garantizando el acceso seguro y controlado a los recursos de datos.	Seguridad de acceso, control de identidades, cumplimiento normativo.	Estonia: e-Residency e ID-Kaart. India: Asdhaar.
Soluciones de telecomunicaciones para la soberanía de datos	Redes	Proyectos para asegurar que los datos de usuarios de telecomunicaciones se mantengan bajo control nacional.	Seguridad de datos, privacidad de usuarios, cumplimiento regulatorio.	Proyectos de Huawei en China, AT&T en EE. UU, Cryptpad en Francia, Proton Mail en Suiza, Matrix en Alemania

Solución Tecnológica	Campo de Aplicación	Descripción	Aspecto clave	Ejemplos y referencias
Tecnologías de Anonimización y Pseudonimización para el cumplimiento de la soberanía de datos	Ciberseguridad	Herramientas que transforman datos personales en datos anónimos, permitiendo su uso sin comprometer la privacidad.	Privacidad, seguridad de datos, cumplimiento normativo.	ARX Data Anonymization Tool, IBM Data Privacy Passports.
Blockchain para Trazabilidad y Cumplimiento	Tecnologías de información	Uso de tecnologías de blockchain para asegurar la trazabilidad de los datos utilizados en IA y verificar el cumplimiento normativo.	Seguridad de datos y cumplimiento normativo.	IBM Food Trust
Frameworks para el cumplimiento de la soberanía de datos	Tecnologías de información	Herramientas que ayudan a las organizaciones a seguir y cumplir con las regulaciones de soberanía de datos.	Seguimiento normativo, auditoría, gestión de cumplimiento	OneTrust, TrustArc

Solución Tecnológica	Campo de Aplicación	Descripción	Aspecto clave	Ejemplos y referencias
Infraestructura de Clave Pública (PKI) para garantizar el cumplimiento de la soberanía de datos	Ciberseguridad	Sistemas que utilizan certificados digitales y criptografía para asegurar la comunicación y la autenticación de datos.	Autenticación, integridad de datos, seguridad de comunicación	DigiCert, Sectigo, GOV.UK Verify (Reino Unido) Bundesnetzagentur (Alemania), eIDAS (Unión Europea)
Iniciativas para la soberanía de los datos sanitarios	Tecnologías de información	Iniciativas para garantizar que los datos de salud de los pacientes se almacenen y procesen dentro del país de origen.	Privacidad de pacientes, seguridad de datos, cumplimiento normativo.	NHS Digital en el Reino Unido, Health Information Exchange en la UE.
Cifrado de Datos para el cumplimiento de la soberanía de datos	Ciberseguridad	Uso de técnicas de cifrado para proteger los datos en tránsito y en reposo, asegurando que solo las entidades autorizadas puedan acceder a ellos.	Seguridad de datos, privacidad, integridad de datos.	Vormetric Data Security by Thales

En la sección siguiente, tal como se describe en la tabla comparativa (ver Tabla 4), aclaramos las soluciones tecnológicas que se han ejecutado y que están actualmente en funcionamiento:

5.1 Infraestructura de Nube Soberana

5.1.1 Espacio de Datos: Los espacios de datos a nivel de infraestructura pueden mejorar significativamente la soberanía y la seguridad de los datos. Al permitir el intercambio seguro de datos entre clústeres gestionados por diferentes actores, estos espacios de datos garantizan que los datos solo sean accesibles para las partes autorizadas y estén protegidos contra el robo. Este enfoque se alinea con la creciente necesidad de cumplir con las normas de protección de datos. Transferir las aplicaciones del consumidor de datos al clúster productor de datos puede alinearse con los patrones de gravedad de los datos.

Esta estrategia se propone para mejorar la eficiencia general del sistema al reducir la necesidad de mover grandes volúmenes de datos entre redes [40]. Existen dos retos clave para habilitar espacios de datos: 1) interoperabilidad de los datos, 2) generación de valor de los datos [55].

En los ecosistemas empresariales, especialmente en los que se intercambian datos sensibles y críticos, el *control del uso* es crucial para mantener la soberanía de los datos. Garantiza que los proveedores de datos puedan hacer cumplir sus políticas sobre la forma en que los consumidores utilizan sus datos, incluso después de haberlos compartido [66].

***Control de Uso*:** El control de uso (UC) se refiere a los mecanismos y políticas que rigen la forma en que se pueden usar los datos una vez que se ha accedido a ellos o se han compartido. A diferencia del control de acceso tradicional, que se centra en sí un usuario puede acceder a los datos, el control de uso se extiende a las acciones que se pueden realizar en los datos una vez que se concede el acceso [66].

Con estos dos aportes para la infraestructura de nubes soberanas, se empezaron a crear espacios de datos especializados, de los cuales destacan los siguientes:

Gaia-X

Gaia-X fue presentado como un proyecto en el 2019 por los Ministerios de Economía de Alemania y Francia y Enero 2024 es recibida por el Parlamento Europeo de Gaia-X

[109], esta solución representa una iniciativa europea dedicada al establecimiento de una infraestructura de datos segura y federada que tiene como objetivo garantizar la soberanía digital en Europa [10], mejorando así la interoperabilidad y los esfuerzos de colaboración entre los proveedores y usuarios de datos, Gaia-X desempeña un papel fundamental en el ecosistema del espacio de datos europeo al facilitar la soberanía de los datos empresariales y fomentar el intercambio de datos entre las empresas europeas. Esto se considera un motor para impulsar la economía digital y crear valor compartido dentro de los ecosistemas industriales.

La estructura consiste en dos ecosistemas principales:

- Ecosistema de infraestructura: abarca la prestación de servicios de infraestructura esenciales para el almacenamiento, la transferencia y el procesamiento de datos [10].
- Ecosistema de datos: se concentra en facilitar los espacios de datos y los servicios avanzados en varios sectores industriales verticales [10].

Gaia-X también se centra en promover la utilización de datos mediante el diseño de incentivos que fomenten el intercambio de datos y la colaboración. Esto implica crear un entorno altruista y mecanismos de intercambio y retroalimentación, que son cruciales para reducir los costos de transacción y fomentar la innovación. En conjunto, Gaia-X personifica un avance fundamental hacia el establecimiento de un ecosistema digital seguro y eficiente en Europa, que promueve la soberanía de los datos y la colaboración en varios sectores.

IDSA (Asociación Internacional de Espacios de Datos)

Propósito y función: La IDSA es una organización clave que participa en el desarrollo de los espacios de datos internacionales (IDS), que están diseñados para facilitar el intercambio de datos soberanos dentro de los ecosistemas empresariales. La IDSA desempeña un papel crucial a la hora de establecer normas empresariales y directrices arquitectónicas de alto nivel que son esenciales para atraer a las empresas a participar en la visión de la IDS [10].

Colaboración con GAIA-X: IDSA colabora con el proyecto GAIA-X, que es otra importante iniciativa europea destinada a crear una infraestructura de datos segura y federada. En conjunto, estos esfuerzos forman parte de una estrategia europea más amplia para mejorar la soberanía digital y la interoperabilidad en el intercambio de datos IDS [10].

Desarrollo de una arquitectura de referencia: IDSA ha desarrollado una arquitectura de referencia que proporciona una descripción de las funciones en los espacios de datos desde una perspectiva empresarial. Estas funciones incluyen el propietario de datos, el proveedor de datos, el consumidor de datos y el proveedor de aplicaciones de datos. Esta arquitectura está diseñada para facilitar el intercambio seguro de datos y la gobernanza dentro de los ecosistemas empresariales, garantizando la soberanía de los datos para todos los participantes. La arquitectura de la IDSA admite un enfoque federado, que es crucial para garantizar la seguridad y la protección de los datos. Participación de la industria: Los esfuerzos de la IDSA cuentan con el respaldo de representantes de varios sectores, incluidas las empresas de software de integración empresarial y el sector logístico holandés. Estas partes interesadas contribuyen a perfeccionar la arquitectura y a evaluar su posible aceptación, especialmente entre las pequeñas y medianas empresas (PYMES) IDS [10].

Centrarse en la soberanía digital: Un tema central del trabajo de IDSA es la soberanía digital, que se refiere a la capacidad de las organizaciones para controlar sus datos e infraestructura digital. Al establecer un marco para el intercambio de datos seguro y soberano, IDSA tiene como objetivo capacitar a las empresas para que mantengan el control sobre sus datos mientras participan en los espacios de datos internacionales IDS [10].

Hay otras propuestas como ***RENA (Reference Enterprise Architecture)*** un marco diseñado para abordar los desafíos de la soberanía de los datos y la interoperabilidad empresarial dentro de los espacios de datos internacionales (IDS). Proporciona un enfoque estructurado para que las empresas desarrollen componentes organizativos y de software que se ajusten a los principios del IDS y, al mismo tiempo, respondan a las necesidades empresariales específicas [22].

Catena-X se basa en los principios de Gaia-X, que implican desarrollar los servicios básicos necesarios y permitir la negociación de contratos para el intercambio de datos y las políticas de uso. Este marco apoya el sistema de apoyo a la toma de decisiones al proporcionar información crítica sobre la composición y el estado de los vehículos, sus componentes y materiales [42].

5.1.2 Cooperativas de Datos:

Una cooperativa de datos es un modelo colaborativo en el que individuos u organizaciones se unen para agrupar sus recursos de datos. El objetivo principal es garantizar un intercambio de datos seguro, confiable y soberano, que pueda empoderar a las comunidades y a las pequeñas y medianas empresas (PYMES) al proporcionarles

un acceso fácil y asequible a la información. Este modelo permite a los participantes negociar colectivamente las decisiones relacionadas con los datos, promoviendo los derechos digitales y el bienestar de la comunidad [11].

Las cooperativas de datos desempeñan un papel crucial en los ecosistemas digitales al proporcionar acceso a la infraestructura que sustenta la economía moderna. Ayudan a preservar los derechos de propiedad y evitan la privatización y la monopolización de los recursos digitales, lo que puede erosionar la autodeterminación, especialmente en un mundo cada vez más mediado por la inteligencia artificial (IA) [11].

Hay varios ejemplos en el mundo de utilización de este tipo de solución de tecnologías como: *Cooperativa Bávara de Datos* sobre la construcción en Alemania es un ejemplo de cooperativa de datos; *eKutir* es una empresa social de la India que utiliza tecnologías digitales para capacitar a los pequeños agricultores con asesoramiento agrícola basado en datos, acceso a la financiación y vínculos con los mercados; *Farmerline*, una empresa ghanesa de tecnología agrícola, proporciona a los pequeños agricultores información agrícola oportuna a través de la tecnología móvil. Este caso ejemplifica el potencial de las cooperativas de datos para mejorar el desarrollo sostenible y la seguridad alimentaria en las zonas rurales y otros [11].

También se han creado soluciones similares en diferentes países que tienen como objetivo el cumplimiento de la soberanía de datos, como:

China: TianYanCha

Tianyancha es una plataforma de servicios gubernamentales y comerciales en China que proporciona acceso a una base de datos masiva de registros corporativos y gubernamentales. Es una herramienta crucial para la transparencia y la supervisión, controlada por las autoridades chinas (actualmente no se tiene acceso a este sitio web desde el extranjero).

Estonia: X-Road

X-Road es la columna vertebral de la infraestructura digital de Estonia, que permite el intercambio seguro de datos entre entidades públicas y privadas. Estonia es conocida por su enfoque avanzado en gobierno digital, y X-Road asegura que los datos personales y transaccionales se mantengan seguros y bajo control nacional.

UK: SOLID

La plataforma SOLID (Social Linked Data) es una iniciativa promovida por Tim Berners-Lee, el creador de la World Wide Web, cuyo propósito es devolver a los usuarios el control sobre sus datos personales. En esencia, SOLID busca transformar la forma en que se manejan los datos en la web mediante un modelo descentralizado de almacenamiento de información. SOLID refuerza este principio al permitir que los usuarios tengan control sobre dónde se almacenan sus datos, quién puede acceder a ellos y cómo se usan.

También hay **opciones privadas** como Nextcloud [141], OwnCloud [144], Infomaniak Network [124], Open Nebula y otros que permiten el alojamiento de archivos, calendarios y otras aplicaciones con control total.

5.2 Geofencing de Datos

El geofencing de datos se refiere a la práctica de usar límites geográficos para controlar el acceso, la transmisión y el uso de los datos. Este concepto está estrechamente relacionado con la localización de datos, que es un enfoque político en el que los países imponen restricciones a los flujos de datos para proteger los datos nacionales al garantizar que se almacenen y procesen dentro de sus fronteras geográficas. La localización de datos puede manifestarse de diversas formas, como el almacenamiento local de datos, la protección de datos y la privacidad de los datos por geolocalización, entre otras [61].

MapSafe está diseñado para abordar la creciente necesidad de privacidad geográfica y soberanía de los datos, especialmente a la luz de las filtraciones de datos de alto perfil y de la comercialización de los datos de los usuarios. Permite a los propietarios de datos soberanos (SDO: “sovereign data owner”) controlar la divulgación de sus datos geográficos confidenciales [53], sus características son:

- Funcionalidad: La herramienta es una aplicación web cliente que ofusca los conjuntos de datos mediante técnicas como el enmascaramiento en forma de rosquilla o el agrupamiento hexagonal. Estos métodos ayudan a proteger los datos al alterar su representación antes de compartirlos [53].
- Cifrado y compartición: MapSafe implementa un esquema de cifrado de varios niveles. Esto permite a los SDoS compartir la información geoespacial cifrada según su criterio y con un nivel de detalle con el que se sientan cómodos. Esto garantiza que los datos permanezcan seguros y bajo el control del propietario de los datos [53].

- Verificación de autenticidad: Para verificar la autenticidad de los datos compartidos, MapSafe almacena el valor hash del volumen cifrado en la cadena de bloques. Este registro público inmutable garantiza que los datos no se hayan manipulado, lo que proporciona un nivel adicional de seguridad y confianza [53].
- Integración y adopción: La herramienta está diseñada para integrarse fácilmente en los sistemas web geoespaciales actuales y futuros, promoviendo su adopción y garantizando que la privacidad geográfica se mantenga en varias plataformas [53].
- Control y soberanía: Al poner la privacidad geográfica bajo el control de los guardianes de los datos, MapSafe garantiza que la decisión de divulgar datos geográficos confidenciales recaiga en los propietarios legítimos, reforzando así el concepto de soberanía de los datos [53].

API de geofencing de Google: Facilita la integración de las capacidades de geofencing en las aplicaciones de Android, lo que mejora el desarrollo de experiencias de usuario centradas en la ubicación [115].

Foursquare: Ofrece un conjunto de herramientas destinadas a la creación de iniciativas de marketing geolocalizadas y al análisis exhaustivo de los datos basados en la ubicación [106].

Radar: Ofrece soluciones de geofencing para aplicaciones móviles, que abarcan funcionalidades como el seguimiento en tiempo real, la geocodificación y el análisis de datos [148].

Airship: Ofrece notificaciones automáticas y servicios de mensajería integrados en la aplicación basados en el geofencing, que se utilizan ampliamente en las estrategias de marketing [69].

5.3 Sistemas de Identificación Digital Nacionales

Estonia: e-Identity

Estonia es pionera en la identificación digital con su tarjeta de identidad electrónica (ID-Card) y el programa e-Residency. El ID-card permite a los ciudadanos estonios acceder a servicios públicos, firmar documentos digitalmente y votar en línea. El programa e-Residency permite a no residentes obtener una identidad digital estonia para gestionar negocios en línea dentro de la UE [97].

India: Aadhaar

Es el sistema de identificación digital más grande del mundo, gestionado por la Autoridad de Identificación Única de la India (UIDAI). Asigna un número único de 12 dígitos a cada ciudadano indio, vinculado a sus datos biométricos. Aadhaar se utiliza para acceder a una amplia gama de servicios públicos y privados, desde subsidios hasta la apertura de cuentas bancarias.

Suecia: BankID

Es el sistema de identificación digital más utilizado en Suecia, desarrollado por bancos en colaboración con el gobierno. Permite a los ciudadanos autenticar su identidad para acceder a servicios gubernamentales, bancarios, firmar documentos y realizar transacciones en línea de manera segura [71]. Noruega tiene un sistema similar.

Finlandia: Finnish Authentication Service (Suomi.fi)

El sistema Suomi.fi en Finlandia ofrece una identificación digital segura que permite a los ciudadanos acceder a servicios gubernamentales, firmar documentos y realizar transacciones en línea. El servicio es parte de la plataforma más amplia Suomi.fi, que centraliza todos los servicios electrónicos públicos en un solo portal.

Bélgica: eID

La tarjeta de identidad electrónica (eID) de Bélgica permite a los ciudadanos acceder a servicios gubernamentales, firmar documentos digitalmente y verificar su identidad en línea. Está vinculada a un chip que almacena los datos personales y de autenticación del usuario, asegurando la seguridad en las transacciones digitales [73].

Singapur: SingPass

Es el sistema de autenticación digital utilizado en Singapur, que permite a los ciudadanos y residentes permanentes acceder a servicios gubernamentales y realizar transacciones en línea. SingPass también permite la autenticación en aplicaciones privadas a través de su integración con el ecosistema digital del país [159].

Australia: myGovID

Es un sistema de identificación digital en Australia que permite a los ciudadanos acceder a servicios gubernamentales en línea. Está diseñado para reemplazar las contraseñas con un sistema más seguro basado en autenticación multifactorial [118].

En estos ejemplos de sistemas de identificación que nos muestra varios tipos de tecnologías utilizadas para identificar al ciudadano, muchos países han implementado

similares sistemas que buscan mejorar la seguridad y facilitar el acceso a servicios públicos, que apoyen en el cumplimiento de la soberanía de datos y la protección de la privacidad.

5.4 Soluciones de telecomunicaciones para la soberanía de datos

Redes Privadas y Seguras:

- China Mobile 5G: China ha impulsado el desarrollo de su propia infraestructura 5G para reducir la dependencia de proveedores extranjeros [87].
- Redes 5G europeas: La Unión Europea está promoviendo la adopción de redes 5G con estrictos controles sobre la ubicación de los datos, bajo regulaciones como el GDPR, para evitar el acceso no autorizado fuera de sus fronteras [146].

Redes Nacionales de Telecomunicaciones:

- Rusia - RuNet: Rusia ha desarrollado una "internet soberana" que permite desconectar el país del resto de la red global si es necesario, asegurando que las comunicaciones internas permanezcan bajo control soberano [76].
- Irán - Intranet Nacional: Irán también ha creado una red interna conocida como la "Red Nacional de Información" para garantizar la independencia de las comunicaciones dentro de sus fronteras [74].

Centro de Datos y Redes locales:

- **Europa - OVHcloud:** es uno de los proveedores de servicios de nube que priorizan el cumplimiento con el GDPR y la soberanía de datos dentro de Europa [143].
- **Brasil – Centro de Datos:** El país ha invertido en centros de datos locales para asegurar que los datos críticos, especialmente aquellos relacionados con servicios financieros y gubernamentales, permanezcan bajo control local [135].

Redes Gubernamentales:

- GovNet (Reino Unido): Una red de comunicaciones seguras diseñada específicamente para el uso del gobierno británico, asegurando que las comunicaciones gubernamentales se mantengan protegidas dentro de su jurisdicción.
- En España la red SARA Network (Sistema de Aplicaciones y Redes para las Administraciones) es una infraestructura de telecomunicaciones que conecta a todas las administraciones públicas en España. Proporciona un entorno seguro para el

intercambio de información y el acceso a servicios comunes, garantizando la soberanía y seguridad de los datos [99].

Soluciones de Redes para Gobiernos:

- Cisco Webex para Gobiernos: Proporciona soluciones de videoconferencia y colaboración en línea con cifrado avanzado, diseñado para cumplir con regulaciones estrictas de soberanía de datos [158].
- Microsoft Teams para Gobierno: Ofrece servicios de comunicaciones y colaboración para gobiernos con almacenamiento de datos controlado y bajo normativas locales [132].

5.5 Tecnologías de Anonimización y Pseudonimización para el cumplimiento de la soberanía de datos

- ***Aircloak Insights Aircloak Insights*** es una solución de anonimización que permite el análisis de datos personales sin comprometer la privacidad. Utiliza una técnica llamada "anonimización diferencial" que garantiza que la información divulgada no revele detalles específicos sobre ningún individuo en particular [68].
- ***Anonos*** es una plataforma que ofrece seudonimización dinámica para proteger la privacidad de los datos mientras se permite su uso en análisis y procesamiento. Esta tecnología permite que los datos sean procesados sin revelar la identidad original de los individuos, cumpliendo con las exigencias de privacidad [70].

5.6 Blockchain para Trazabilidad y Cumplimiento

- **IBM Food Trust:** Utiliza blockchain para rastrear el origen y la trazabilidad de los alimentos a lo largo de la cadena de suministro, asegurando que cada paso del proceso cumpla con los estándares de calidad y soberanía de datos [120].
- **Civic:** Es una plataforma basada en blockchain que permite la gestión de identidades digitales de forma segura y descentralizada. Los usuarios tienen control total sobre sus datos personales, lo que asegura que cumplan con las regulaciones de soberanía [82].

5.7 Plataformas para el cumplimiento de la soberanía de datos

- ***India: DIGIT (Digital Infrastructure for Governance, Impact, and Transformation)***

DIGIT es una plataforma de código abierto que sirve como base para desarrollar aplicaciones de gobierno electrónico en India. Está diseñada para ayudar a los gobiernos locales a implementar soluciones digitales que se ajusten a sus necesidades, manteniendo el control sobre los datos y asegurando la escalabilidad y adaptabilidad [93].

- ***Rusia: Gosuslugi***

  Gosuslugi es un portal único de servicios gubernamentales en Rusia, que permite a los ciudadanos acceder a servicios estatales y municipales en línea. Está diseñado para asegurar que los datos personales y transaccionales permanezcan bajo la jurisdicción rusa y cumplan con las normativas de protección de datos del país [117].

- ***Canadá: GCcollab y GCconnex***

  GCcollab y GCconnex son plataformas de colaboración y redes sociales internas del gobierno canadiense. Estas herramientas están diseñadas para facilitar la colaboración entre los empleados gubernamentales mientras se garantiza que los datos sensibles se manejen dentro de un entorno seguro y controlado por el gobierno (solo tienen acceso empleados gubernamentales).

- ***Australia: myGov***

  myGov es un portal centralizado que permite a los ciudadanos australianos acceder a servicios gubernamentales en línea, como el pago de impuestos, atención médica y servicios sociales. El portal está diseñado para mantener los datos dentro de la jurisdicción australiana y bajo estrictos controles de seguridad [119].

- ***Brasil: e-Governe***

  e-Governe es un conjunto de soluciones integradas diseñadas para modernizar la administración pública, ofreciendo herramientas para la gestión de salud, educación, finanzas, y otros sectores gubernamentales. Es una plataforma que permite a los gobiernos locales y nacionales gestionar sus operaciones de manera eficiente, con un alto grado de control sobre los datos [77].

- ***Estados Unidos:* OpenGov**

  OpenGov es una plataforma para la administración financiera, la transparencia y la participación ciudadana en gobiernos locales. Ofrece herramientas para la planificación presupuestaria, la rendición de cuentas y la gestión de datos financieros, permitiendo un control exhaustivo sobre la información [142].

5.8 Infraestructura de Clave Pública (PKI) para garantizar el cumplimiento de la soberanía de datos

- **eIDAS (Unión Europea):** El reglamento de identificación electrónica y servicios de confianza (eIDAS) de la UE establece estándares para la autenticación electrónica

y las firmas digitales, utilizando PKI para asegurar que las transacciones electrónicas transfronterizas cumplan con las leyes de soberanía de datos de cada estado miembro [102]**.**

- **España** cuenta con un sólido sistema de certificados digitales que permite a los ciudadanos acceder en línea a los servicios de la Administración, presentar impuestos y gestionar la Seguridad Social y otros trámites oficiales. Los certificados los expide la Fábrica Nacional de Moneda y Timbre (FNMT) [139].
- **DocuSign** es una plataforma que permite a empresas y particulares firmar documentos electrónicamente, automatizar acuerdos y gestionar digitalmente todo el ciclo de vida de los contratos. Se utiliza ampliamente para firmas electrónicas seguras y legalmente vinculantes, y ayuda a agilizar el proceso de preparación, firma y gestión de contratos en diversos sectores, como el financiero, el sanitario y el inmobiliario. Utilizado por varios países como Estados Unidos, Francia, Alemania, Australia, Chile y otros [95].

5.9 Iniciativas para la soberanía de los datos sanitarios

MiData (Suiza); es una cooperativa suiza que ofrece una plataforma donde los ciudadanos pueden gestionar y controlar sus propios datos de salud de manera segura. Este modelo pone a los pacientes en el centro, dándoles control sobre quién tiene acceso a su información de salud [137].

Objetivos:

- Empoderar a los ciudadanos suizos para que sean los custodios de sus datos sanitarios [137].
- Dar la seguridad que los datos sanitarios se almacenen y procesen dentro de Suiza, bajo las leyes suizas de protección de datos [137].
- Facilitar el intercambio de datos de salud de manera segura y bajo el consentimiento informado de los ciudadanos [137].

La plataforma facilita la investigación médica al permitir a los ciudadanos compartir voluntariamente sus datos con investigadores, siempre bajo sus propias condiciones [137].

National Health Data System (Francia); Francia ha implementado un sistema nacional de datos de salud denominado Health Data Hub. Este sistema centraliza los datos sanitarios del país para su uso en investigación y desarrollo de políticas públicas [151].

Objetivos:

- Crear un repositorio centralizado de datos sanitarios que esté bajo control del estado francés [151].
- Facilitar la investigación médica y el desarrollo de nuevas terapias al proporcionar acceso a datos sanitarios de manera regulada y controlada [151]
- Hay que asegurar que los datos sanitarios franceses permanezcan dentro de Francia y se manejen conforme a las leyes francesas [151].

El Health Data Hub promueve la soberanía de los datos sanitarios al garantizar que todos los datos clínicos estén centralizados bajo una infraestructura francesa, cumpliendo con la normativa local. Facilita el acceso a datos para la investigación, bajo estrictos controles de privacidad y seguridad [151].

My Health Record (Australia); es un sistema nacional de registros de salud electrónico en Australia. Todos los ciudadanos australianos tienen un registro de salud digital que contiene su historial médico [94].

Objetivos:

- Proporcionar a los ciudadanos australianos acceso a su historial médico en cualquier momento, manteniendo los datos bajo control australiano [94].
- Facilitar la interoperabilidad entre diferentes sistemas de salud en el país, asegurando que los datos se compartan solo dentro de las fronteras australianas [94].
- Proteger los datos sanitarios conforme a las leyes de privacidad y seguridad de Australia [94].

My Health Record asegura que los datos sanitarios se manejen dentro de Australia, lo que refuerza la soberanía nacional sobre estos datos. Los ciudadanos tienen control sobre su información, pudiendo decidir quién puede acceder a sus registros médicos [94].

También hay soluciones tecnológicas como “The Ignyte Assurance Platform” [145] y otras.

5.10 Cifrado de Datos para el cumplimiento de la soberanía de datos

- ***Protegrity Data Security Platform;*** ofrece una plataforma integral de seguridad de datos que incluye cifrado, tokenización y técnicas de anonimización. Esta solución

permite a las organizaciones cumplir con normativas de soberanía de datos y proteger la información sensible en todo su ciclo de vida [153].

- ***Vormetric Data Security by Thales;*** es una solución de cifrado y tokenización que permite proteger datos sensibles, tanto en reposo como en movimiento. Es utilizada por organizaciones para asegurar que los datos cumplan con las normativas de soberanía y privacidad de datos [154].

5.11 Software de apoyo al cumplimiento de leyes de soberanía de datos

- ***En el caso de ejemplos gubernamentales:***

  En España:

  Gestiona-RGPD; añadiendo funcionalidades para la identificación del riesgo, medidas de mitigación y capacidad para la gestión de múltiples tratamientos de alto y escaso riesgo para dar respuesta a las obligaciones del RGPD en materia de gestión del riesgo, registro de actividades de tratamiento, inventario de tratamiento y medidas de seguridad [89].

  ***Válida-Cripto RGPD*;** donde se vienen a trasladar los criterios de la guía para facilitar la gestión los requisitos de cifrado de los tratamientos de datos personales con un enfoque eminentemente práctico, dando así respuesta a las consultas que en ocasiones se realizan a la AEPD con relación a la validez o no de los sistemas criptográficos sobre cuyos requisitos corresponde al responsable tomar las decisiones adecuadas para proteger los datos de los interesados seguridad [89].

  Asesora-Brecha y Comunica-Brecha; dotando a estas herramientas de capacidad para emitir informes que pueden ser utilizados como documentación para demostrar cumplimiento seguridad [89].

  Emprende; herramienta para ayudar a los emprendedores y startups tecnológicas a cumplir con la normativa de protección de datos seguridad [89].

  Facilita RGPD, herramienta para facilitar la adecuación al RGPD de empresas y profesionales seguridad [89].

  En la Unión Europea:

GDPR checklist: Nuestra lista de comprobación del GDPR puede ayudarle a asegurar su organización, proteger los datos de sus clientes y evitar costosas multas por incumplimiento [133].

- ***En el caso de ejemplos empresas privadas:***

  Las grandes empresas tecnológicas han implementado varias herramientas que ayudan a cumplir con las leyes de soberanía de datos, por ejemplo:

  AWS: Amazon Macie.

  Microsoft: Purview.

  Google: Google Cloud Platform (GCP).

  Otras empresas privadas también han desarrollado herramientas comerciales como:

  TrustArc; esta completa suite de soluciones orientadas al GDPR ayuda a las empresas a planificar, implementar, actualizar y mantener el cumplimiento del GDPR. Sus funciones principales incluyen la presentación de informes a los reguladores, la supervisión del cumplimiento y el registro de las actividades procesadas [155].

  Didomi; se trata de otro sistema de gestión de consentimientos y preferencias muy extendido en el mercado que permite recopilar, almacenar y configurar los permisos y preferencias de los usuarios en consecuencia. También puede evaluar la puntuación de cumplimiento de su empresa en porcentaje [92].

Capítulo 6: Recomendaciones Prácticas

6.1 Directrices y Estrategias generales recomendadas:

i. Conocimiento y comprensión de las legislaciones locales sobre Normativas de Protección de datos.
ii. Inventariar y clasificar los datos.
iii. Fomentar la localización de datos dentro de la jurisdicción.
iv. Establecer o hacer uso de tratados internacionales que regulen el acceso y tratamiento de datos.
v. Implementaciones de Medidas de Seguridad como Encriptación, controles de accesos, Detección de intrusos, Planes de respuestas a incidentes, cifrados y tecnologías de seguridad.
vi. Autonomía Digital para minimizar la dependencia de plataformas extranjeras para la gestión de datos personales y sensibles.
vii. Transparencia y comunicación informando a los ciudadanos o usuarios de cómo se recopila, utiliza y protegen sus datos.
viii. Obtener el consentimiento explícito de los interesados antes de procesar sus datos.
ix. Permitir que el interesado tenga el derecho de acceso, rectificación, eliminar y oponerse al uso de sus datos personales.
x. Auditorias de los proveedores externos en procesado de datos de acuerdo con las leyes y normas nacionales de privacidad y seguridad.
xi. Requerimientos a los proveedores de certificaciones de cumplimiento entregadas por las instituciones responsables de la gobernanza de los datos.
xii. Contratos que establezcan cláusulas contractuales claras y detalladas que establezcan responsabilidades de cada parte en protección de los datos.
xiii. Educación y concientización fomentando la importancia de la soberanía de los datos y los niveles de responsabilidades de las entidades, empresas e individuos.
xiv. Las transferencias de datos entre instituciones o fuera de la jurisdicción debe cumplir con las legislaciones federadas, nacionales o locales.
xv. Tener en cuenta la protección de los datos desde el diseño y desarrollo de los productos y servicios digitales.
xvi. Constante evaluación del impacto en la protección de datos para mitigar los riesgos asociados a nuevos proyectos de tratamientos de datos.

xvii. Mejora continua de todos los componentes involucrados en el cumplimiento de la soberanía de datos.

6.2 Guías para implementación del cumplimiento de la soberanía de datos

En esta sección, presento guías rápidas para los organismos gubernamentales, las corporaciones, las pequeñas y medianas empresas (PYMES) y los individuos; que les permitirán ejecutar las medidas necesarias para cumplir con las regulaciones vigentes que hacen cumplir la soberanía de los datos, teniendo en cuenta el contexto y las circunstancias geográficas.

En la investigación que he realizado he podido encontrar guías e instrucciones propuestas para la protección y privacidad de la data, para la transferencia de datos y otras; pero no he podido encontrar una especialmente para implementar la soberanía de datos, por lo que propongo las siguientes:

6.2.1 Guías para Entidades Gubernamentales:

1. Auditoría de Datos

Identificar datos críticos: Determina qué tipo de datos maneja la entidad (ciudadanos, políticas públicas, financieros, etc.).

Clasificar datos: Define qué información es sensible y debe estar protegida bajo normativas estrictas.

2. Cumplimiento Normativo

Normativas nacionales e internacionales: Asegura el cumplimiento de las leyes locales de protección de datos (por ejemplo, Ley de Protección de Datos Personales) y considera normativas internacionales relevantes.

Designar un Responsable de Datos: Nombrar un Oficial de Protección de Datos (DPO) para asegurar el cumplimiento y la vigilancia de las normativas.

3. Políticas de Localización de Datos

Almacenamiento en servidores nacionales: Mantén los datos de los ciudadanos en centros de datos dentro del país para evitar conflictos con normativas extranjeras.

Infraestructura propia o en la nube gubernamental: Prioriza el uso de centros de datos locales y nubes específicas para entidades gubernamentales.

4. Medidas de Seguridad

Cifrado avanzado: Aplica cifrado de extremo a extremo tanto en la transmisión como en el almacenamiento de los datos.

Autenticación multifactor (MFA): Implementa MFA para todas las plataformas que manejan datos sensibles.

Monitoreo continuo: Utiliza herramientas para detectar y mitigar amenazas en tiempo real.

5. Gestión de Proveedores y Contratos

Evaluar proveedores externos: Asegura que todos los proveedores de servicios tecnológicos cumplan con las normativas locales de protección de datos y seguridad.

Firmar Acuerdos de Procesamiento de Datos (DPA): Establece contratos claros que definan responsabilidades en el manejo y procesamiento de datos.

6. Plan de Respuesta ante Incidentes

Establecer un plan de respuesta a brechas de datos: Crea un protocolo claro para gestionar violaciones de seguridad, incluyendo medidas para contener el daño y restaurar los servicios.

Notificación inmediata: Diseñar un procedimiento para notificar a las autoridades pertinentes y a los ciudadanos afectados por una fuga de datos.

7. Capacitación del Personal

Formación en seguridad y soberanía de datos: Capacita a todo el personal gubernamental en las mejores prácticas para proteger la información y evitar brechas.

Conciencia cibernética: Promueve una cultura de protección y responsabilidad en el manejo de datos sensibles.

8. Políticas de Acceso y Gobernanza

Acceso basado en roles (RBAC): Establece que solo los empleados con roles específicos puedan acceder a ciertos datos, reduciendo el riesgo de acceso no autorizado.

Gobernanza de datos: Define claramente quién es responsable de qué información y cómo se puede usar.

9. Monitoreo y Auditoría Continua

Auditorías regulares: Realiza auditorías periódicas para asegurar que las políticas de soberanía de datos se están cumpliendo.

Evaluación y ajuste: Actualiza las políticas según los cambios tecnológicos, normativos y las lecciones aprendidas.

10. Conclusión y Beneficios

Cumplimiento normativo: Garantizar la seguridad de los datos de los ciudadanos y el cumplimiento con las normativas de soberanía de datos.

Protección de la confianza pública: Salvaguardar la integridad de los datos sensibles y mejorar la confianza de los ciudadanos en las instituciones gubernamentales.

6.2.2 Guía para Corporaciones:

1. Auditoría Inicial de Datos

Identificación de datos críticos: Identifica qué datos maneja la empresa (clientes, empleados, financieros, propiedad intelectual).

Clasificación de datos: Clasifica la información según su nivel de sensibilidad (por ejemplo, datos personales, estratégicos, o financieros).

2. Cumplimiento Normativo

Revisión de leyes locales e internacionales: Cumple con las normativas aplicables como la Ley de Protección de Datos local, GDPR, CCPA u otras regulaciones según el país o región en la que operes.

Asignación de un Responsable de Datos: Nombra un Oficial de Protección de Datos (DPO) para supervisar el cumplimiento de las normativas y proteger los datos.

3. Políticas de Localización de Datos

Almacenamiento local o en la nube regulada: Asegúrate de que los datos sensibles se almacenen dentro de la jurisdicción nacional o en plataformas que cumplan con las normativas locales.

Requisitos de proveedores en la nube: Verifica que los proveedores de almacenamiento en la nube ofrezcan opciones de localización de datos y cumplan con las leyes locales de soberanía de datos.

4. Medidas de Seguridad

Cifrado robusto: Utiliza cifrado de extremo a extremo tanto en los datos almacenados como en tránsito.

Autenticación multifactor (MFA): Implementa MFA en todos los sistemas que manejan datos sensibles para garantizar la seguridad.

Monitorización de acceso: Implementa sistemas de monitoreo para detectar accesos no autorizados y vulnerabilidades.

5. Gestión de Proveedores y Terceros

Evaluación de proveedores: Realiza una auditoría de proveedores para asegurarte de que cumplan con las normativas de protección de datos y seguridad.

Acuerdos de procesamiento de datos (DPA): Formaliza contratos con terceros que especifiquen las responsabilidades de cada parte en el manejo de los datos.

6. Políticas de Acceso y Control

Acceso basado en roles (RBAC): Limita el acceso a los datos según el rol del empleado, asegurando que solo el personal autorizado pueda acceder a información crítica.

Privacidad por diseño: Asegúrate de que las plataformas y aplicaciones utilizadas estén diseñadas con la protección de la privacidad como prioridad desde su desarrollo.

7. Plan de Respuesta ante Incidentes

Plan de contingencia ante fugas de datos: Diseña un plan claro para gestionar y contener posibles brechas de seguridad, y establecer protocolos para la restauración de servicios.

Notificación de incidentes: Define cómo y cuándo notificar a los afectados y a las autoridades pertinentes en caso de una fuga de datos.

8. Capacitación del Personal

Capacitación en seguridad de datos: Ofrece capacitación regular a todos los empleados sobre cómo manejar y proteger los datos de manera segura.

Concienciación sobre la protección de datos: Promueve una cultura organizacional donde la seguridad de los datos sea una prioridad para todos los niveles de la empresa.

9. Monitoreo y Auditoría Continua

Auditorías periódicas: Realiza revisiones y auditorías regulares de la infraestructura y políticas de datos para asegurarte de que se están siguiendo las mejores prácticas.

Ajustes y actualizaciones: Mantén las políticas de seguridad actualizadas conforme a las nuevas normativas, tecnologías y amenazas emergentes.

10. Beneficios y Conclusiones

Protección de la empresa y clientes: Salvaguardar los datos sensibles reduce el riesgo de sanciones y daños a la reputación.

Confianza de los clientes: Garantizar la privacidad y seguridad de los datos aumenta la confianza de los clientes y fortalece la reputación de la empresa.

Cumplimiento regulatorio: Cumplir con las normativas evita sanciones legales y asegura una operación más sólida y segura.

6.2.3 Guía para PYMES:

1. Evaluación Inicial de Datos

Identificar los tipos de datos: ¿Qué datos manejas? (clientes, empleados, financieros, transacciones).

Clasificar los datos: Define qué datos son sensibles (por ejemplo, datos personales, información financiera) y deben tener protección adicional.

2. Cumplimiento Legal

Revisar leyes locales de protección de datos: Cumple con la legislación aplicable, como la Ley de Protección de Datos Personales o el GDPR (si operas en la UE).

Asignar un responsable: Designa a una persona dentro de la empresa que se encargue de supervisar la protección de datos (aunque no sea necesario un DPO, alguien debe ser responsable).

3. Almacenamiento de Datos

Usar proveedores de confianza: Asegúrate de que los servicios en la nube o almacenamiento que utilices cumplan con las normativas locales y ofrezcan medidas de protección de datos adecuadas.

Mantener el control de datos críticos: Siempre que sea posible, almacena los datos sensibles en servidores locales o en proveedores que te permitan tener el control sobre su ubicación.

4. Medidas de Seguridad

Cifrado de datos: Asegúrate de que los datos estén cifrados, tanto en tránsito (cuando se envían) como en reposo (cuando se almacenan).

Autenticación multifactor (MFA): Utiliza MFA para acceder a los sistemas y plataformas más sensibles.

Actualizaciones de seguridad: Mantén siempre actualizados los sistemas de seguridad y antivirus para protegerte contra amenazas.

5. Acceso y Control

Control basado en roles: Limita el acceso a los datos según el rol del empleado; no todos necesitan acceso a toda la información.

Contraseñas seguras: Asegúrate de que los empleados utilicen contraseñas seguras y únicas para sus cuentas.

6. Gestión de Proveedores

Seleccionar proveedores con políticas de protección de datos: Cuando trabajes con terceros, verifica que sigan prácticas adecuadas de seguridad y protección de datos.

Establecer acuerdos claros: Asegúrate de que los contratos con terceros incluyan cláusulas de seguridad de datos y cumplimiento normativo.

7. Plan de Respuesta a Incidentes

Desarrollar un plan básico: Define los pasos a seguir si hay una brecha de seguridad o fuga de datos (por ejemplo, notificación a clientes y autoridades).

Notificación rápida: En caso de una violación de datos, notifícalo lo antes posible a los clientes afectados y a las autoridades regulatorias.

8. Capacitación y Concienciación

Capacitación básica en protección de datos: Asegúrate de que todos los empleados entiendan cómo manejar datos de manera segura.

Promover la concienciación: Fomenta una cultura en la que la protección de datos sea responsabilidad de todos.

9. Monitoreo y Revisión

Auditorías periódicas: Revisa regularmente cómo se están manejando los datos en la empresa y si se están siguiendo las políticas de seguridad.

Actualización de políticas: Revisa y ajusta tus políticas de protección de datos conforme surjan nuevas leyes o amenazas.

10. Conclusiones y Beneficios

Protección contra riesgos: Implementar medidas de seguridad adecuadas protege a tu PyME de sanciones, pérdida de reputación y costosos incidentes de seguridad.

Cumplimiento normativo: Asegurar el cumplimiento legal evita multas y protege la confianza de tus clientes.

Fomentar la confianza: La protección efectiva de datos genera confianza entre tus clientes y fortalece tu reputación como negocio.

6.2.4 Guía para Individuos:

1. Auditoría Personal de Datos

Identifica tus datos personales: Haz una lista de qué información compartes (nombre, dirección, cuentas bancarias, datos de salud, etc.).

Clasifica los datos sensibles: Determina qué información es más importante proteger (contraseñas, números de identificación, información financiera).

2. Control del Almacenamiento de Datos

Almacena datos sensibles en lugares seguros: Utiliza servicios en la nube que ofrezcan cifrado y privacidad, o guarda información sensible en discos duros externos y cifrados.

Evita servicios no confiables: No almacenes información importante en plataformas que no garantizan la seguridad y el control sobre los datos.

3. Uso de Contraseñas Seguras

Utiliza contraseñas fuertes y únicas: Asegúrate de que tus contraseñas sean largas, complejas, y diferentes para cada servicio.

Gestor de contraseñas: Considera utilizar un gestor de contraseñas para generar y almacenar contraseñas seguras sin necesidad de recordarlas todas.

4. Autenticación Multifactor (MFA)

Activa la autenticación multifactor: Habilita MFA en todas las cuentas que lo ofrezcan (bancos, correos electrónicos, redes sociales) para agregar una capa adicional de seguridad.

5. Cifrado de Datos

Cifrado en dispositivos: Activa el cifrado en tus dispositivos (teléfonos, computadoras) para proteger la información en caso de robo o pérdida.

Cifrado en servicios de mensajería: Usa aplicaciones de mensajería que ofrezcan cifrado de extremo a extremo (como Signal o WhatsApp).

6. Gestión de Privacidad en Redes Sociales

Revisa la configuración de privacidad: Ajusta la configuración en redes sociales para controlar quién puede ver tu información y publicaciones.

Minimiza la exposición: Evita compartir información sensible (como ubicaciones, números de identificación, etc.) en plataformas públicas.

7. Gestión de Datos con Terceros

Selecciona aplicaciones y servicios confiables: Antes de instalar una aplicación o registrarte en un servicio, revisa su política de privacidad para saber cómo manejan tus datos.

Revoca permisos innecesarios: Revisa qué permisos has otorgado a las aplicaciones y elimina los que no sean necesarios (como acceso a la cámara o contactos).

8. Navegación Segura en Internet

Utiliza un navegador seguro: Usa navegadores que respeten tu privacidad, como Brave o Firefox, y activa bloqueadores de anuncios para reducir el seguimiento.

Red privada virtual (VPN): Considera usar una VPN para cifrar tu conexión y evitar que terceros rastreen tu actividad en línea.

9. Monitorización y Alerta de Actividad Sospechosa

Configura alertas en tus cuentas: Activa notificaciones en tus cuentas bancarias o de servicios críticos para recibir alertas de actividades inusuales.

Revisa regularmente tu información: Monitorea tus estados financieros y cuentas para detectar posibles accesos no autorizados o actividades sospechosas.

10. Plan de Respuesta ante Robo de Datos

Ten un plan para incidentes: Si sospechas que tus datos han sido comprometidos, actúa rápidamente para cambiar contraseñas y contactar a las entidades involucradas (bancos, servicios).

Alerta a las autoridades: Si experimentas una violación grave, considera alertar a las autoridades locales o agencias de protección de datos.

6.3 Validación

Para fundamentar las directrices antes mencionadas, llevamos a cabo una revisión exhaustiva de los estudios académicos que se han realizado en relación con los criterios o requisitos previos que deben cumplirse para la integración en los marcos regulatorios establecidos para validar la soberanía de los datos en sus diversos dominios.

6.3.1 Listado de requisitos para integrar la soberanía de datos

- ✓ **Implementación de tecnologías:** Para permitir la soberanía de los datos y el consentimiento informado, es crucial implementar tecnologías como los sistemas de gestión del consentimiento digital, las tecnologías que preservan la privacidad y las herramientas de cuantificación del riesgo de privacidad. Estas tecnologías ayudan a gestionar el consentimiento de forma granular y a proteger la privacidad de los datos de los pacientes [45].
- ✓ **Diseño de usabilidad e interacción:** El software debe cumplir con los estándares de diseño de usabilidad e interacción. Esto garantiza que la tecnología sea fácil de usar y no abrume a los usuarios con información compleja, lo que favorece el consentimiento informado [45].
- ✓ **Aceptación y confianza del usuario:** Es vital cumplir con los criterios relacionados con la aceptación y la confianza de los usuarios. Esto incluye la participación de los usuarios en el proceso de investigación, especialmente cuando se utilizan sus datos, para fomentar la transparencia y la confianza [45].
- ✓ **Participación de los usuarios:** Es crucial garantizar una participación rigurosa de los usuarios, especialmente si los datos se donan con fines de investigación. Esta participación ayuda a alinear las prácticas de investigación con las expectativas de los usuarios y los estándares éticos [45].
- ✓ **Reglas técnicas y no técnicas:** Los requisitos incluyen normas técnicas y no técnicas para la gestión de datos. Esto abarca la eliminación, el procesamiento y la persistencia de los datos, lo que garantiza que los datos se manejen adecuadamente durante todo su ciclo de vida [45]. Las detallo por ser importantes visualizarlas:
    - *Eliminación y persistencia de datos;* las normas técnicas dictan los métodos y tecnologías utilizados para la eliminación y la persistencia de los datos. Por ejemplo, se deben implementar métodos específicos de eliminación de datos para cumplir con normativas como el RGPD, que exige el derecho al olvido. Las normas no técnicas, como las políticas organizativas, garantizan que estos

métodos técnicos se apliquen de forma coherente y transparente en toda la organización.

- *Transparencia y consentimiento del usuario*; las normas no técnicas exigen que las organizaciones mantengan la transparencia con los usuarios sobre cómo se procesan y almacenan sus datos. Esto implica obtener el consentimiento de los usuarios e informarles sobre las actividades de localización y procesamiento de datos. Las normas técnicas respaldan este objetivo mediante la implementación de sistemas que rastrean y administran las actividades de procesamiento de datos y de consentimiento de los usuarios, garantizando que estos procesos sean auditables y cumplan con los requisitos legales.
- *Aplicación de políticas;* las normas técnicas implican la implementación de mecanismos de aplicación de políticas, como los controles de acceso y las técnicas de anonimización de datos. Las normas no técnicas, por otro lado, definen las políticas que deben aplicarse, como quién puede acceder a los datos y en qué condiciones. En conjunto, garantizan que los datos se utilicen de conformidad con las políticas de la organización y las normativas legales.
- *Requisitos específicos del dominio*; en algunos sectores, se necesitan requisitos técnicos específicos, como los mecanismos de cifrado y firma, para cumplir con las normas legales y reglamentarias. Las normas no técnicas garantizan que estas soluciones técnicas estén alineadas con los estándares del sector y los requisitos legales, y proporcionan un marco para su implementación y uso.

✓ **Propiedad y control:** Las organizaciones deben establecer claramente la propiedad y el control de sus datos. Esto incluye la capacidad de tomar decisiones con respecto a los activos de datos y hacer cumplir las condiciones de uso para el intercambio de datos. Los proveedores de datos deben poder realizar un seguimiento del uso de los datos y determinar dónde se almacenan sus datos, ya sea en una metaplataforma, en su infraestructura o en la infraestructura del consumidor de datos [147].

✓ **Medidas de Seguridad:** La implementación de medidas de seguridad sólidas es esencial para evitar el acceso no autorizado, la alteración de los datos y las fallas del sistema durante las transacciones de intercambio de datos. Deben existir funciones de seguridad actualizadas para proteger la integridad y confidencialidad de los datos [147].

✓ **Control de acceso:** Garantizar que solo los usuarios autorizados tengan acceso a los datos es un requisito fundamental. Esto implica implementar mecanismos que permitan a los usuarios controlar quién puede ver o usar sus recursos de datos [9].

✓ **Calidad de los datos**: Los datos de alta calidad son esenciales para una soberanía efectiva de los datos. La mala calidad de los datos puede socavar los beneficios de

la soberanía de los datos, por lo que es crucial mantener datos precisos y confiables [9].

- ✓ **Localización de datos:** Algunas jurisdicciones exigen que los datos se almacenen dentro de las fronteras del país. El cumplimiento de estos requisitos implica la creación de centros de datos locales o el uso de servicios en la nube que ofrezcan opciones de localización de datos [60].
- ✓ **Posesión y protección de los datos:** Para cumplir con la soberanía de los datos, una entidad debe poseer los datos y tener la capacidad de protegerlos contra diversas amenazas, como las violaciones de datos, el robo de identidad y el terrorismo de datos. Esto implica implementar medidas de seguridad sólidas para garantizar la integridad y confidencialidad de los datos [59].
- ✓ **Cumplimiento reglamentario:** El cumplimiento de las leyes y reglamentos de acuerdo con la jurisdicción geográfica en la que se ubique la entidad o individuo, es un requisito fundamental. Estas regulaciones suelen motivar las prácticas de intercambio de datos y establecen el marco legal dentro del cual las organizaciones deben operar [29]. Un ejemplo es el «derecho al olvido» de la Unión Europea, que exige la eliminación o restricción de los datos personales cuando se soliciten [59].
- ✓ **Transparencia y consentimiento del usuario:** Es crucial garantizar la transparencia sobre la localización, el procesamiento y el derecho a la eliminación de los datos. Las organizaciones deben asegurarse de que los usuarios finales estén informados y estén de acuerdo con la forma en que se gestionan sus datos en los distintos productos y servicios [29].
- ✓ **Responsabilidad de los involucrados:** Es crucial definir claramente las responsabilidades de todas las partes involucradas en el intercambio de datos. Las metaplataformas deben seleccionar a los participantes que cumplan con las normas de intercambio de datos y asumir la responsabilidad en caso de uso indebido o robo de datos confidenciales. Esto garantiza que todas las partes conozcan sus funciones y puedan ser consideradas responsables del manejo de los datos [147].
- ✓ **Cumplimiento de las regulaciones**: Los proveedores de datos deben estar informados sobre las leyes y reglamentos pertinentes para evitar infracciones. Deben contar con procedimientos técnicos para responder a estas leyes y utilizar mecanismos de resolución de controversias para gestionar los conflictos con los consumidores de datos en caso de que surjan [147].
- ✓ **Derechos de desistimiento:** los proveedores de datos deben poder retirar sus datos de los participantes de una metaplataforma o mercado de datos si es necesario. Esto garantiza que mantengan el control sobre sus datos y que puedan actuar si la soberanía de sus datos se ve comprometida [147].

- ✓ **Control de uso:** los usuarios deben poder adjuntar políticas de uso específicas a sus datos. Esto significa que pueden decidir cómo otros utilizan sus datos y asegurarse de que se ajusten a sus preferencias de privacidad y seguridad [9].
- ✓ **Cumplimiento organizativo**: las organizaciones deben alinear sus políticas y procedimientos internos con los requisitos de soberanía de los datos. Esto incluye garantizar que las prácticas de administración de datos cumplan tanto con los estándares internos como con los reglamentos externos [9].
- ✓ **Políticas de gobierno de datos**: Es vital establecer políticas claras de gobierno de datos que describan cómo se recopilan, almacenan, procesan y comparten los datos. Estas políticas deben revisarse y actualizarse periódicamente para reflejar los cambios en las leyes y la tecnología [60].
- ✓ **Transferencias de datos transfronterizas:** Al transferir datos a través de las fronteras, las organizaciones deben asegurarse de que dichas transferencias cumplen con los acuerdos y marcos internacionales de transferencia de datos, como los de la UE y EE. UU. Escudo de privacidad o cláusulas contractuales estándar [60].
- ✓ **Monitoreo y adaptación:** Dada la naturaleza dinámica de las leyes de soberanía de datos, las organizaciones deben monitorear continuamente los desarrollos legales y adaptar sus estrategias de cumplimiento en consecuencia. Esto implica mantenerse informadas sobre los cambios en las regulaciones y actualizar las prácticas de administración de datos para alinearlas con los nuevos requisitos [54].
- ✓ **Marco de gobierno de datos**: Establecer un marco sólido de gobierno de datos es crucial para garantizar el cumplimiento continuo. Esto incluye políticas y procedimientos para el manejo de datos, auditorías periódicas y capacitación para los empleados sobre las leyes de protección de datos y privacidad. El marco basado en gráficos de conocimientos que se propone en el documento puede ayudar a gestionar estos aspectos al ayudar a clasificar los datos e identificar las leyes aplicables [54].
- ✓ **Auditorías y actualizaciones regulares:** Realice auditorías periódicas para garantizar el cumplimiento de los requisitos legales en evolución y actualizar las políticas y prácticas en consecuencia [6].
- ✓ **Intercambio de datos y colaboración:** Además de proteger los datos, las entidades también deben facilitar el intercambio de datos y la colaboración con socios de confianza. Esto implica establecer acuerdos claros de intercambio de datos y garantizar que los datos se compartan de forma segura y responsable [59].
- ✓ **Monetización de los datos**: Comprender el valor de los datos y cómo se pueden monetizar sin dejar de mantener la soberanía es otro requisito clave. Esto implica

crear estrategias que permitan un intercambio rentable de datos sin comprometer el control [9].

- ✓ **Derechos de portabilidad de los datos:** El cumplimiento exige habilitar el derecho a la portabilidad de los datos, lo que permite que los datos se transfieran fácilmente entre diferentes sistemas y fronteras. Esto es crucial para facilitar el libre flujo de datos y maximizar su valor económico [59].
- ✓ **Defensa estratégica y alianzas:** Formar alianzas con otros soberanos de datos puede mejorar la protección y el cumplimiento. Este enfoque colectivo puede proporcionar beneficios económicos y de seguridad mejorados, como la ubicación conjunta de los servidores en centros de datos seguros para optimizar el uso de los recursos y las estrategias de defensa [59].
- ✓ **Utilización económica de los datos:** El cumplimiento también implica reconocer los datos como un recurso económico y aprovecharlos para el crecimiento económico. Esto incluye el desarrollo de productos de datos que puedan reemplazar las tareas manuales y contribuir a la economía de datos global [59].
- ✓ **Transferencias proactivas y estratégicas:** Las entidades deben realizar transferencias proactivas y estratégicas de los derechos de datos cuando sea necesario. Esto implica negociar acuerdos de intercambio de datos que se alineen con los objetivos de la organización y anticipar las posibles amenazas u oportunidades [59].

6.3.2 Categorización de Requisitos:

Clasificaremos sistemáticamente en la Tabla 5, los diversos requisitos en función de las dimensiones específicas que se han delineado en el marco del capítulo de Fundamento Teórico, que abarca las siguientes categorías:

A. Dominio Sociotécnico: enfoque técnico, social, ético y de derechos humanos.
B. Dominio Legal: enfoque legal, político y de gobernanza de datos.
C. Dominio económico: enfoque económico.

TABLA 5: CUADRO DE REQUERIMIENTOS VS. DOMINIOS

Requerimientos / Dominios	Sociotécnico	Legal	Económico
Implementación de tecnologías	X		
Diseño de usabilidad e interacción	X		
Aceptación y confianza del usuario	X		
Participación de los usuarios	X		

Reglas técnicas y no técnicas	X	X	
Propiedad y control	X		
Medidas de Seguridad	X		
Control de acceso	X		
Localización de datos	X	X	
Calidad de los datos	X		
Posesión y protección de los datos	X	X	
Cumplimiento reglamentario		X	
Transparencia y consentimiento del usuario	X	X	
Responsabilidad de los involucrados	X	X	
Cumplimiento de las regulaciones	X	X	
Derechos de desistimiento	X	X	
Control de uso	X	X	
Cumplimiento organizativo		X	
Políticas de gobierno de datos	X	X	
Transferencias de datos transfronterizas	X	X	
Monitoreo y adaptación	X		
Marco de gobierno de datos		X	
Auditorías y actualizaciones regulares		X	
Intercambio de datos y colaboración	X		
Monetización de los datos			X
Derechos de portabilidad de los datos	X	X	X
Defensa estratégica y alianzas		X	X
Utilización económica de los datos	X		X
Transferencias proactivas y estratégicas	X	X	X
Total	**23**	**17**	**5**

6.3.3 Validación

Para validar rigurosamente el cumplimiento de las estipulaciones establecidas en los requisitos de soberanía de datos, cuantificaremos meticulosamente el número de requisitos específicos que se hayan cumplido satisfactoriamente en cada dominio individual, lo que nos permitirá obtener el porcentaje de cumplimiento pertinente para cada dominio, lo que posteriormente nos permitirá agregar estos hallazgos para determinar el nivel promedio general de cumplimiento en todos los dominios combinados. Para esto proponemos este cuadro de resultados en la Tabla 6.

TABLA 6: RESULTADO DE EVALUACIÓN PARA EL CUMPLIMIENTO DE LA SOBERANÍA DE DATOS

Evaluación	Sociotécnico	Legal	Económico
Cumple	# requerimientos cumplidos	# requerimientos cumplidos	# requerimientos cumplidos
No Cumple	# requerimientos no cumplidos	# requerimientos no cumplidos	# requerimientos no cumplidos
% de Cumplimiento	(#req. cumplidos/23) *100	(#req. cumplidos/17) *100	(#req. cumplidos/5) *100

La evaluación que sugiero no abarca las características que un software debe cumplir para mantener la soberanía de los datos. En relación con esto, encontré una publicación académica [43] en donde los autores detallaban los requisitos funcionales y no funcionales; para un sistema de intercambio de datos que cumple con los requisitos para el cumplimiento de la soberanía de datos (ver anexo 3).

6.3.4 Prueba

Caso práctico

En una organización retail, la fusión de la soberanía de los datos y la promulgación de políticas que garanticen el cumplimiento de los marcos regulatorios relacionados con la gestión de la información confidencial se ha incluido en la cartera de proyectos de TI. Esto constituye una estrategia esencial para salvaguardar la privacidad de los clientes y fomentar la confianza en la marca, al tiempo que se mitiga el riesgo de las repercusiones legales que pueden derivarse de un manejo inadecuado de los datos. La ejecución de estas políticas requiere no solo la adopción de tecnologías adecuadas, sino también la formación del personal sobre la importancia de la seguridad de la información y las respuestas conductuales necesarias. Con este fin, nos ceñiremos a un marco de mejores prácticas que abarque los protocolos de seguridad, las estrategias de respuesta a los incidentes y las evaluaciones periódicas de los riesgos. Además, se fomentará una cultura organizacional que priorice la protección de datos, fomentando la responsabilidad colectiva entre todos los empleados y estableciendo vías de comunicación explícitas para denunciar cualquier irregularidad.

El equipo Project Manager tendrá la responsabilidad de supervisar la implementación de estas medidas, garantizando que cada departamento cumpla con los estándares establecidos y se mantenga informado sobre los últimos avances en ciberseguridad.

Se realizó como práctica la implementación de la Guía para una Empresa (ver Anexo 4), de este instrumento y de la información recolectada al realizar esta Guía podemos

realizar la evaluación del cumplimiento de la Empresa de la soberanía de datos. A continuación, hacemos esta evaluación:

Evaluación	Sociotécnico	Legal	Económico
Cumple	15	8	2
No Cumple	8	9	3
% de Cumplimiento	(15/23) *100=**65,2%**	(8/17) *100=**47,0%**	(2/5) *100=**40%**

Los resultados indican que la empresa está logrando avances significativos en la incorporación del cumplimiento de la soberanía de los datos en sus enfoques y metodologías tecnológicas. Esto no solo mejora la confianza de los clientes, sino que también refuerza su posición en el mercado internacional.

Capítulo 7: Conclusiones

7.1 Resumen de lo encontrado

Con base en la investigación realizada, se han identificado los aspectos clave esenciales para comprender esta área de estudio, que abarcan una comprensión clara de la definición de soberanía de datos, las leyes y regulaciones que la rigen, junto con las soluciones tecnológicas que ofrece en un mundo cada vez más digitalizado.

Al principio de esta investigación, se descubrió que la ***definición de soberanía de datos*** a menudo se confunde con términos como «soberanía digital», «soberanía de la información» y otras expresiones similares. Esto indica la ambigüedad que prevalece en la literatura con respecto a cómo definir estos conceptos y sus repercusiones en los ámbitos legal y tecnológico. En este contexto, se encontró varias perspectivas que examinan la soberanía de los datos desde diferentes perspectivas, como la protección de la privacidad, la regulación del flujo de información y la responsabilidad de las plataformas digitales. En consecuencia, se logró identificar las sutilezas entre estos términos, lo que permitió comprender mejor cómo cada uno de ellos se relaciona con la autonomía de los estados a la hora de supervisar sus datos y la necesidad de establecer marcos regulatorios claros.

Al mismo tiempo, esto ayudo a reducir el concepto de ***soberanía de los datos a su contexto aplicable*** para salvaguardar los derechos de los ciudadanos en un panorama digital cada vez más complejo, en el que las autoridades reguladoras competentes deben colaborar con las empresas de tecnología para mantener un equilibrio entre la innovación y la protección de la información personal. La soberanía de los datos, como se ha mencionado, está intrínsecamente ligada a la geografía y a los acuerdos o tratados que los estados establecen. Esta variabilidad en su aplicación significa que la forma en que se implementan las regulaciones sobre la soberanía de los datos puede diferir significativamente de un país a otro. Por lo tanto, es crucial que los estados trabajen en conjunto con las empresas y los ciudadanos para crear un marco que no solo proteja los derechos de los individuos, sino que también fomente un entorno justo y confiable. Los acuerdos internacionales pueden facilitar la cooperación entre naciones, asegurando que las plataformas digitales operen de manera responsable y que la información personal de los ciudadanos esté protegida. Al mismo tiempo, estos marcos deben adaptarse a las particularidades culturales y legales de cada región, lo que subraya la importancia de un enfoque contextualizado en la regulación de la soberanía de los datos. En resumen, un equilibrio entre la innovación tecnológica y la protección

de la información personal es esencial para garantizar que todos los actores involucrados se beneficien de un entorno digital seguro y equitativo.

En cuanto a las ***leyes y reglamentos***, el 77% de los países han establecido normas para el cumplimiento de la protección de datos, la mayoría de las cuales se alinean con las directrices del GDPR y los estándares de la OCDE, lo que resulta en una mayor armonización de la legislación mundial. Por el contrario, países como China, Rusia, Irán y otros han adoptado medidas más estrictas, haciendo hincapié en la autoridad estatal por encima de la privacidad personal, lo que ha creado tensiones internacionales y ha planteado desafíos para las empresas que operan en diversas jurisdicciones. Mientras tanto, Estados Unidos ha adoptado un enfoque más desarticulado, con leyes que difieren mucho entre los estados, lo que complica aún más las cosas para las organizaciones que intentan cumplir con las normas de protección de datos. Al mismo tiempo, las naciones europeas han tratado de crear un espacio unificado, respaldado y dirigido por la Unión Europea, lo que ha llevado a la promulgación del Reglamento General de Protección de Datos (GDPR), que establece puntos de referencia más altos para la privacidad y la seguridad de los datos personales. Esto ha fomentado un entorno en el que las empresas deben adaptarse rápidamente a las diversas regulaciones, lo que puede resultar caro y complejo, especialmente para las que carecen de los recursos necesarios para sortear las complejidades legales. Otros países, como Australia, siguen manteniendo una legislación más indulgente, lo que ha suscitado debates sobre la eficacia de las regulaciones y su influencia en la innovación y el comercio internacional. Entre los 149 países cuyos marcos regulatorios se examinan, observamos una distinción entre los continentes maduros y los emergentes, donde las naciones en desarrollo suelen encontrar obstáculos adicionales para establecer políticas eficaces que protejan la información sin obstaculizar el progreso económico, como ocurre en América Latina y algunos países africanos que se esfuerzan por equilibrar la protección de datos con la necesidad de atraer inversiones extranjeras. Esto subraya la necesidad de crear marcos que no solo sean sólidos sino también adaptables, que permitan a las empresas adaptarse a un panorama global en constante evolución. El concepto de crecimiento sostenible debe ir acompañado de la innovación regulatoria, cultivando un ecosistema en el que la confianza de los consumidores y la competitividad empresarial puedan prosperar juntas.

Las ***soluciones tecnológicas*** disponibles en el mercado son variadas y abarcan desde infraestructuras en la nube hasta herramientas analíticas que permiten a las empresas cumplir con las regulaciones y, al mismo tiempo, mantener su agilidad. Se ha clasificado por tipos y áreas de aplicación, lo que ayuda a identificar los sectores en los que se está

produciendo el desarrollo, a saber, las tecnologías de la información, las redes y la ciberseguridad. Entre las áreas con mayor potencial y avance en lo que respecta a la integración de nuevas normativas se encuentran los espacios de datos, softwares especializados en gestionar políticas de privacidad y seguridad de los datos, software para gestionar el consentimiento y las auditorías automatizadas, todas las cuales facilitan el cumplimiento de la normativa y aumentan la confianza de los consumidores. Además, hay sectores en los que la especialización se ha vuelto más pronunciada; como la salud, la industria, la administración gubernamental y la economía de datos; donde la adopción de estas tecnologías no solo agiliza los procesos, sino que también fomenta una mayor transparencia y responsabilidad en la gestión de la información. Además, la colaboración entre sectores es vital, ya que facilita el intercambio de mejores prácticas y la creación de estándares comunes que refuerzan la seguridad y la privacidad en la gestión de datos. Este enfoque no solo beneficia a las organizaciones, sino que también empodera a las personas al otorgarles un mayor control sobre su información personal y fomentar una cultura que respeta la privacidad. El ciudadano medio aún no ha desarrollado una cultura de uso responsable de los datos, lo que subraya la importancia de la educación y la concienciación sobre los riesgos y beneficios de la digitalización; sin embargo, los datos encontrados en la investigación indican un interés creciente en la protección de los datos personales, junto con las iniciativas destinadas a informar y empoderar a la población sobre cómo gestionar su información de forma segura.

7.2 Contribuciones

Las contribuciones que he realizado a través de este trabajo se centran en fortalecer la aplicación de la soberanía de los datos como un medio adicional para empoderar a las personas, permitiéndoles ejercer un mayor control sobre su información personal y, al mismo tiempo, fomentar una atmósfera en la que se estime y proteja la privacidad. Esto se logra proporcionando ***información práctica*** sobre su significado, identificando las leyes y regulaciones esenciales que deben cumplirse, los derechos que poseen las personas y las prácticas óptimas para administrar los datos en el panorama digital. Al hacer referencia a las soluciones tecnológicas ya establecidas en varias organizaciones, es evidente que estas iniciativas no solo sirven a los intereses de los usuarios, sino que también fomentan la confianza en las plataformas digitales. Además, esto implica articularlo en guías que sean fáciles de seguir y enumerar los requisitos clave que deben cumplirse para alinearse con la soberanía de los datos.

7.3 Limitaciones

Los desafíos que podemos enfrentar en la implementación práctica de la soberanía de los datos abarcan varias perspectivas multidisciplinarias, que van desde los *factores políticos* hasta la *disponibilidad de los recursos económicos y tecnológicos* necesarios para su ejecución. Abordar estos problemas requiere un enfoque colaborativo entre los gobiernos, las empresas y la sociedad civil para desarrollar un marco que no solo proteja la privacidad de los ciudadanos, sino que también fomente la innovación y el progreso sostenible en el panorama digital. La cooperación entre estas entidades es crucial para el establecimiento de marcos teóricos y prácticos que faciliten el desarrollo de políticas eficientes y adaptables, capaces de abordar los rápidos avances tecnológicos y las necesidades cambiantes de la población. El ámbito sigue siendo dinámico y evoluciona en cierta medida en función de los acuerdos forjados entre las partes interesadas, lo que, posteriormente, puede aumentar la confianza y la inversión en soluciones digitales innovadoras. La inversión y la priorización son cada vez más vitales debido a las nuevas tecnologías emergentes que están revolucionando nuestra interacción con el medio ambiente y la gestión de nuestros recursos, incluidas la inteligencia artificial generativa, blockchain y la IoT. Estos avances no solo ofrecen oportunidades para mejorar la eficiencia, sino que también introducen dilemas éticos y de seguridad que exigen atención inmediata. Hasta que no se logre una estandarización consensuada entre las naciones del mundo que ayude a proteger los datos de sus ciudadanos y, al mismo tiempo, permita un crecimiento continuo en conjunto, será difícil aprovechar al máximo las capacidades de estas tecnologías. La cooperación global se vuelve imperativa para crear marcos regulatorios que fomenten la innovación responsable y garanticen el desarrollo sostenible.

7.4 Trabajos futuros

En esta sección se propone realizar las siguientes investigaciones sobre la integración de la soberanía de datos en el contexto de la globalización y el avance tecnológico, analizando cómo las políticas actuales afectan la privacidad y la seguridad de la información, los cuales son:

- Aportar de manera colaborativa y participativa, abogando por la formulación de directrices destinadas a establecer un marco regulatorio que aborde adecuadamente las exigencias que plantean las tecnologías emergentes y sus ramificaciones en materia de privacidad, seguridad y consideraciones éticas, garantizando así que los avances en la tecnología generen beneficios para la sociedad en su conjunto. Persisten numerosas preguntas sin resolver sobre la

IA generativa, la computación de vanguardia, el Internet de las cosas (IoT), la tecnología blockchain y otras innovaciones; en consecuencia, existe una necesidad apremiante de un discurso sostenido entre los legisladores, los especialistas en tecnología y el público.

- Realización de estudios empíricos adicionales para examinar el impacto combinado de factores como la propiedad, el control, la seguridad, el cumplimiento y la responsabilidad en la soberanía de los datos, especialmente dentro de la intrincada gobernanza de los metaplataformas.
- La formulación de contratos inteligentes que garanticen la interoperabilidad entre mercados interconectados representa una estrategia viable para mejorar la soberanía de los datos y fomentar la confianza entre los usuarios y las plataformas. Además, es imperativo desarrollar marcos regulatorios que no solo salvaguarden la privacidad de los datos, sino que también faciliten la innovación y el desarrollo sostenible en un panorama digital en constante evolución.
- Refinar los marcos para la evaluación de la soberanía de los datos puede generar directivas más precisas para las organizaciones y promover la integración de metodologías responsables en la administración de la información. Esto abarca el establecimiento de puntos de referencia éticos que dicten la aplicación de tecnologías emergentes, garantizando así que se priorice el bienestar de los usuarios y mitigando los riesgos relacionados con el uso indebido de los datos. Además, es imperativo fomentar las sinergias entre los sectores público y privado para idear soluciones que enfrenten los dilemas de la privacidad y la seguridad, cultivando así un ecosistema en el que la confianza constituya la base de las interacciones digitales. Además, es crucial abogar por la educación y la conciencia sobre la importancia de la soberanía de los datos, empoderando así a las personas para que tomen decisiones sensatas con respecto a sus datos personales.

Referencias Bibliográficas

[1] Aaronson, S. A. (2021). *Data is disruptive: How data sovereignty is challenging data governance*.

[2] Abbas, A. E., Van Velzen, T., Ofe, H., Van De Kaa, G., Zuiderwijk, A., & De Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets*, *34*(1), 20. https://doi.org/10.1007/s12525-024-00695-2

[3] Abdelkarim, Y. A. (2024). A literature review of the evolution of sovereignty and borders concepts in cyberspace. *International Cybersecurity Law Review*, *5*(2), 365-372. https://doi.org/10.1365/s43439-024-00118-0

[4] Altendeitering, M., Pampus, J., Larrinaga, F., Legaristi, J., & Howar, F. (2022). Data sovereignty for AI pipelines: Lessons learned from an industrial project at Mondragon corporation. *Proceedings of the 1st International Conference on AI Engineering: Software Engineering for AI*, 193-204. https://doi.org/10.1145/3522664.3528593

[5] Anastasiadou, I., Beqiraj, D. J., & Gauci, D. J.-P. (2023). *Disaggregation of Digital Information and Data Sovereignty Compliance*.

[6] Appenzeller, A., Balduf, F., & Beyerer, J. (2023). Usability for Data Sovereignty—Evaluation of Privacy Risk Quantification Interfaces. *Proceedings of the 16th International Conference on PErvasive Technologies Related to Assistive Environments*, 206-214. https://doi.org/10.1145/3594806.3594816

[7] Arenas, J. (2021). LFPDPPP. *Journal Law and Economy*, 10-13. https://doi.org/10.35429/JLE.2020.7.4.10.13

[8] Bareh, C. K. (2024). Reviewing the Privacy Implications of Indias Digital Personal Data Protection Act (2023) from Library Contexts. *DESIDOC Journal of Library & Information Technology*, *44*(1), 50-58. https://doi.org/10.14429/djlit.44.1.18410

[9] Biehs, S., & Stilling, J. (2024). *Identification of Key Requirements for the Application of Data Sovereignty in the Context of Data Exchange*.

[10] Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Network*, *35*(2), 4-5. https://doi.org/10.1109/MNET.2021.9387709

[11] Bühler, M. M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Mookerje, V., Nübel, K., Pentland, A., Scholz, T., Siddarth, D., Tait, J., Vaitla, B., & Zhu, J. (2023). Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities. *Digital*, *3*(3), 146-171. https://doi.org/10.3390/digital3030011

[12] Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415-434. https://doi.org/10.1080/09662839.2022.2101885

[13] Calzada, I. (2021). Data Co-Operatives through Data Sovereignty. *Smart Cities*, *4*(3), 1158-1172. https://doi.org/10.3390/smartcities4030062

[14] Chander, A., & Sun, H. (Eds.). (2023). *Data Sovereignty: From the Digital Silk Road to the Return of the State* (1.ª ed.). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197582794.001.0001

[15] Chandra, R., Singh, P., Kumar, S., & Shankar, D. M. (2024). *Geographical Data Sovereignty in the Cloud: A Comparative Analysis of Compliance and Security*. *23*(03).

[16] Cheung, A. S. Y. (2022). From Data Subjects to Data Sovereigns: Addressing the Limits of Data Privacy in the Digital Era. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4218780

[17] Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), tyac011. https://doi.org/10.1093/cybsec/tyac011

[18] Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y., & Choo, K.-K. R. (2019). On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications. *IEEE Internet of Things Journal*, *6*(3), 4521-4535. https://doi.org/10.1109/JIOT.2018.2886410

[19] Falcão, R., Matar, R., Rauch, B., Elberzhager, F., & Koch, M. (2023). A Reference Architecture for Enabling Interoperability and Data Sovereignty in the Agricultural Data Space. *Information*, *14*(3), 197. https://doi.org/10.3390/info14030197

[20] Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435-453. https://doi.org/10.1080/09662839.2022.2102896

[21] Fernandes, M. E., & Nuzzi, A. P. E. (2022). Fundamentos da Lei Geral de Proteção de Dados (LGPD): Uma revisão narrativa. *Research, Society and Development*, *11*(12), e310111234247. https://doi.org/10.33448/rsd-v11i12.34247

[22] Firdausy, D. R., De Alencar Silva, P., Van Sinderen, M., & Iacob, M.-E. (2022). Towards a Reference Enterprise Architecture to enforce Digital Sovereignty in International Data Spaces. *2022 IEEE 24th Conference on Business Informatics (CBI)*, 117-125. https://doi.org/10.1109/CBI54897.2022.00020

[23] Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369-378. https://doi.org/10.1007/s13347-020-00423-6

[24] Galbraith, J. (2020). United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data. *American Journal of International Law*, *114*(1), 124-128. https://doi.org/10.1017/ajil.2019.80

[25] Gao, H. S. (2021). Data Sovereignty and Trade Agreements: Three Digital Kingdoms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3940508

[26] Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C.

(2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919-958. https://doi.org/10.1080/14650045.2022.2050070

[27] Gu, H. (2023). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-023-09855-1

[28] Hellmeier, M. (2023). *A DELIMITATION OF DATA SOVEREIGNTY FROM DIGITAL AND TECHNOLOGICAL SOVEREIGNTY*.

[29] Hellmeier, M., Pampus, J., Qarawlus, H., & Howar, F. (2023). Implementing Data Sovereignty: Requirements & Challenges from Practice. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1-9. https://doi.org/10.1145/3600160.3604995

[30] Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156-174. https://doi.org/10.1080/17579961.2020.1727094

[31] Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

[32] Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 205395172098201. https://doi.org/10.1177/2053951720982012

[33] Hutchinson, J., Stilinovic, M., & Gray, J. E. (2024). Data sovereignty: The next frontier for internet policy? *Policy & Internet*, *16*(1), 6-11. https://doi.org/10.1002/poi3.386

[34] Hutterer, A., & Krumay, B. (2023). *Adoption of data spaces as multi-sided platforms: Towards a preliminary adoption framework (Page Count: 16)*.

[35] Jarke, M. (2020). Data Sovereignty and the Internet of Production. En S. Dustdar, E. Yu, C. Salinesi, D. Rieu, & V. Pant (Eds.), *Advanced Information Systems*

Engineering (Vol. 12127, pp. 549-558). Springer International Publishing. https://doi.org/10.1007/978-3-030-49435-3_34

[36] Jarke, M., Otto, B., & Ram, S. (2019). Data Sovereignty and Data Space Ecosystems. *Business & Information Systems Engineering*, *61*(5), 549-550. https://doi.org/10.1007/s12599-019-00614-2

[37] Kukutai, T. (2024). How Indigenous communities in New Zealand are protecting their data. *Science*, *384*(6691), eado9298. https://doi.org/10.1126/science.ado9298

[38] Lateef, M. A., O. Taiwo, L., & Adeyoju, A. (2022). Examining the Powers of the NITDA to Enforce Data Protection Laws in Nigeria. *Global Privacy Law Review*, 89-97.

[39] Liu, L. (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, *56*(1), 45-67. https://doi.org/10.1007/s12116-021-09319-8

[40] Marino, J., Camiciotti, L., Cheinasso, F., Olivero, A., & Risso, F. (2023). Enabling Compute and Data Sovereignty with Infrastructure-Level Data Spaces. *Proceedings of the 3rd Eclipse Security, AI, Architecture and Modelling Conference on Cloud to Edge Continuum*, 77-85. https://doi.org/10.1145/3624486.3624509

[41] Moraka, L. I., & Singh, U. G. (2023). The POPIA 7th Condition Framework for SMEs in Gauteng. En A. Shukla, B. K. Murthy, N. Hasteer, & J.-P. Van Belle (Eds.), *Computational Intelligence* (pp. 831-838). Springer Nature Singapore.

[42] Mügge, J., Grosse Erdmann, J., Riedelsheimer, T., Manoury, M. M., Smolka, S.-O., Wichmann, S., & Lindow, K. (2023). Empowering End-of-Life Vehicle Decision Making with Cross-Company Data Exchange and Data Sovereignty via Catena-X. *Sustainability*, *15*(9), 7187. https://doi.org/10.3390/su15097187

[43] Pampus, J., & Heisel, M. (2024). An Empirical Examination of the Technical Aspects of Data Sovereignty: *Proceedings of the 19th International Conference on Software Technologies*, 112-122. https://doi.org/10.5220/0012760600003753

[44] Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

[45] Radic, M., Busch-Casler, J., Vosen, A., Herrmann, P., Appenzeller, A., Mucha, H., Philipp, P., Frank, K., Dauth, S., Köhm, M., Orak, B., Spiecker Genannt Döhmann, I., & Böhm, P. (2024). Data sovereignty requirements for patient-oriented AI-driven clinical research in Germany. *Ethik in Der Medizin*. https://doi.org/10.1007/s00481-024-00827-4

[46] Rafik, M. (2021). Data Sovereignty: New Challenges for Diplomacy. En F. Roumate (Ed.), *Artificial Intelligence and Digital Diplomacy* (pp. 33-43). Springer International Publishing. https://doi.org/10.1007/978-3-030-68647-5_3

[47] Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

[48] Roberts, J. S., & Montoya, L. N. (2022). *Decolonisation, Global Data Law, and Indigenous Data Sovereignty* (arXiv:2208.04700). arXiv. http://arxiv.org/abs/2208.04700

[49] Robles Carrillo, M. (2023). La articulación de la soberanía digital en el marco de la Unión Europea. *Revista de Derecho Comunitario Europeo*, *75*, 133-171. https://doi.org/10.18042/cepc/rdce.75.05

[50] Rodríguez, N. M. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[boe n.º 294, de 6-XII-2018]*. *7*.

[51] Ryngaert, C., & Taylor, M. (2020). The GDPR as *Global* Data Protection Regulation? *AJIL Unbound*, *114*, 5-9. https://doi.org/10.1017/aju.2019.80

[52] Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, *10*(1), 1. https://doi.org/10.20956/halrev.v10i1.5016

[53] Sharma, P., Martin, M., & Swanlund, D. (2023). MAPSAFE: A complete tool for achieving geospatial data sovereignty. *Transactions in GIS*, *27*(6), 1680-1698. https://doi.org/10.1111/tgis.13094

[54] Singi, K., Choudhury, S. G., Kaulgud, V., Bose, R. P. J. C., Podder, S., & Burden, A. P. (2020). Data Sovereignty Governance Framework. *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, 303-306. https://doi.org/10.1145/3387940.3392212

[55] Solmaz, G., Cirillo, F., Fürst, J., Jacobs, T., Bauer, M., Kovacs, E., Santana, J. R., & Sánchez, L. (2022). Enabling data spaces: Existing developments and challenges. *Proceedings of the 1st International Workshop on Data Economy*, 42-48. https://doi.org/10.1145/3565011.3569058

[56] Spirkl, C. (2024). Data Laws Around the Globe – Insights, Frictions and Opportunities. Highlights from the African Data Protection Laws Conference in Accra, Ghana, 13-15 September 2022 and Comparative Data Law Conference in Munich, Germany, 7-8 December 2023. *GRUR International*, *73*(9), 865-871. https://doi.org/10.1093/grurint/ikae093

[57] Stéphane Couture, Stephane Couture, Couture, S., Sophie Toupin, & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital?: *New Media & Society*, *21*(10), 2305-2322. https://doi.org/10.1177/1461444819865984

[58] Tai, K., & Zhu, Y. Y. (2022). A historical explanation of Chinese cybersovereignty. *International Relations of the Asia-Pacific*, *22*(3), 469-499. https://doi.org/10.1093/irap/lcab009

[59] Tang, C., Plasek, J. M., Zhu, Y., & Huang, Y. (2020). Data sovereigns for the world economy. *Humanities and Social Sciences Communications*, *7*(1), 184. https://doi.org/10.1057/s41599-020-00664-y

[60] Tao, Y., Yang, S., & Ge, H. (2022). Comparative Study on Data Sovereignty Guarantee Technology. *2022 IEEE 13th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 1-6. https://doi.org/10.1109/PAAP56126.2022.10010593

[61] Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

[62] Vatanparast, R. (2020). Data and the Elasticity of Sovereignty. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3609579

[63] Von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data Sovereignty in Information Systems. *Electronic Markets*, *34*(1), 15. https://doi.org/10.1007/s12525-024-00693-4

[64] Yang, J. (2022). An Overview of the Chinese "Personal Information Protection Law". *Pin Code*, *10*(1), 8-13. Cairn.info. https://doi.org/10.3917/pinc.010.0008

[65] Zhang, L., Cui, Y., & Mu, Y. (2020). Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. *IEEE Systems Journal*, *14*(1), 387-397. https://doi.org/10.1109/JSYST.2019.2911391

[66] Zrenner, J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management*, *32*(3), 477-495. https://doi.org/10.1108/JEIM-03-2018-0058

Referencias Web

[67] Agencias. (02 de 07 de 2024). *La Vanguardia*. Obtenido de https://www.lavanguardia.com/vida/20240702/9776262/gobierno-brasil-prohibe-meta-datos-usuarios-entrenar-modelos-ia-agenciaslv20240702.html#:~:text=S%C3%A3o%20Paulo%2C%202%20jul%20(EFE,de%20inteligencia%20artificial%20(IA).

[68] aircloak. (04 de 09 de 2024). *aircloak*. Obtenido de https://www.aircloak.com/

[69] Airship. (03 de 09 de 2024). *Airship*. Obtenido de https://www.airship.com/

[70] ANONOS. (04 de 09 de 2024). *About Anonos*. Obtenido de https://www.anonos.com/

[71] BankID. (04 de 09 de 2024). *About BankID*. Obtenido de https://www.bankid.com/en/privat/om-bankid

[72] BBC. (2018 de 03 de 2020). *New Mundo BBC*. Obtenido de https://www.bbc.com/mundo/noticias-43472797

[73] beID. (04 de 09 de 2024). *eID software*. Obtenido de https://eid.belgium.be/en/what-eid

[74] Biyani, N. (29 de 08 de 2022). *Internet Society*. Obtenido de https://pulse.internetsociety.org/es/blog/irans-internet-shutdowns-are-facilitated-by-careful-attempts-at-fragmentation-of-the-network

[75] Board, E. D. (13 de 08 de 2024). *RGPD: Directrices, recomendaciones y buenas prácticas*. Obtenido de https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_es

[76] Bonilla, R. S. (13 de 07 de 2023). *Interesa Newtral*. Obtenido de https://www.newtral.es/que-es-runet-internet-de-rusia-que-podria-aislar-a-su-poblacion/20230713/

[77] Brasil, G. d. (04 de 09 de 2024). *e-governe*. Obtenido de http://e-governe.com/#sistemas

[78] Bukaty, P. (2019). *The California Consumer Privacy Act (CCPA): An implementation guide.* United Kingdom: IT Governance Publishing.

[79] Canada, J. L. (13 de 08 de 2024). *Personal Information Protection and Electronic Documents Act*. Obtenido de https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

[80] China, T. N. (15 de 08 de 2024). *Data Security Law of the People's Republic of China*. Obtenido de http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm

[81] China, T. N. (13 de 08 de 2024). *Personal Information Protection Law of the People's Republic of China*. Obtenido de http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

[82] Civic. (05 de 09 de 2024). *Civic Docs*. Obtenido de https://docs.civic.com/integration-guides/civic-pass

[83] Commision, P. I. (15 de 08 de 2024). *Personal Information Protection Commision*. Obtenido de https://www.pipc.go.kr/eng/user/lgp/law/lawsRegulations.do#none

[84] Commisions, F. T. (05 de 2024). *FY 2023 Annual Report.* Obtenido de https://www.ftc.gov/reports/fy-2023-annual-report

[85] Commission, P. D. (14 de 08 de 2024). *PDPA Overview*. Obtenido de https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act

[86] Consult, W. B. (2023). *2023 Global Data Privacy Law Survey Report.* USA: https://info.womblebonddickinson.com/global-data-privacy-law-2023.

[87] Cuesta, A. (14 de 06 de 2023). *Mobile World Live*. Obtenido de https://www.mobileworldlive.com/old_spanish/huawei-se-lleva-el-grueso-del-nuevo-contrato-5g-de-china-mobile/

[88] Datatilsynet. (14 de 08 de 2024). *The Danish Data Protection Agency*. Obtenido de https://www.datatilsynet.dk/

[89] Datos, A. E. (09 de 06 de 2021). *Agencia Española Protección Datos*. Obtenido de https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales/comunicado-privacy-

shield#:~:text=El%2016%20de%20julio%20de,internacionales%20de%20datos%20a%20EEUU.

[90] datos, a. e. (2023). *Memoria Anual.* Madrid.

[91] Datos, A. E. (04 de 09 de 2024). *Listado de herramientas*. Obtenido de https://www.aepd.es/guias-y-herramientas/herramientas

[92] Didomi. (05 de 09 de 2024). *Privacy Requests*. Obtenido de https://www.didomi.io/es/privacy-request

[93] digit.in. (04 de 09 de 2024). *digit.in*. Obtenido de https://www.digit.in/

[94] digitalhealth.gov.au. (05 de 09 de 2024). *For everyone*. Obtenido de https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record

[95] docusign. (05 de 09 de 2024). *About the Guide*. Obtenido de https://www.docusign.com/products/electronic-signature/legality/global

[96] ECONÓMICOS, O. P. (31 de 10 de 2011). *Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. Obtenido de https://www.oecd.org/en/publications/terms-of-reference-for-the-review-of-the-oecd-guidelines-governing-the-protection-of-privacy-and-transborder-data-flows-of-personal-data_5kg2b7l7pljk-en.html

[97] e-Estonia. (04 de 09 de 2024). *e-Identity*. Obtenido de https://e-estonia.com/solutions/estonian-e-identity/id-card/

[98] Empresa, G. (10 de 09 de 2024). *Ayuda relacionada con la Política de consentimiento de usuarios de la Unión Europea.* Obtenido de https://www.google.com/intl/es/about/company/user-consent-policy-help/

[99] España, G. d. (04 de 09 de 2024). *Portal Administración Electrónica*. Obtenido de https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=redsara

[100] Estado, A. E. (10 de 09 de 2024). *Agencia Estatal Boletín Oficial del Estado.* Obtenido de https://www.boe.es/buscar/doc.php?id=DOUE-L-2015-82575

[101] euronews. (10 de 04 de 2022). *euronews*. Obtenido de https://www.euronews.com/next/2022/10/04/ukraine-crisis-russia-amazon

[102] Europea, C. (14 de 10 de 2014). *Preguntas y respuestas: Reglamento sobre identificación electrónica y servicios de confianza (eIDAS)*. Obtenido de https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_586

[103] Europea, C. (26 de 08 de 2024). *Solicitudes de los ciudadanos*. Obtenido de https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_es

[104] Europea, C. E. (10 de 09 de 2024). *Comunicados de Prensa.* Obtenido de https://www.consilium.europa.eu/es/press/press-releases/2024/04/22/eu-japan-council-endorses-the-conclusion-of-the-strategic-partnership-agreement/

[105] eurostat. (26 de 01 de 2024). News articles. *How internet users protected their data in 2023*.

[106] Foursquare. (03 de 09 de 2024). *Foursquare*. Obtenido de https://location.foursquare.com/

[107] FRANCE24. (20 de 07 de 2024). *FRANCE24*. Obtenido de https://www.france24.com/es/programas/econom%C3%ADa/20240720-nigeria-aplic%C3%B3-una-multa-millonaria-a-meta-por-violar-datos-de-los-usuarios

[108] Gaia-X. (27 de 08 de 2024). *Gaia-X*. Obtenido de https://gaia-x.eu/

[109] Gaia-X. (01 de 09 de 2024). *Gaia-X*. Obtenido de https://gaia-x.eu/what-is-gaia-x/about-gaia-x/

[110] GDPR.EU. (05 de 09 de 2024). *GDPR checklist for data controllers*. Obtenido de https://gdpr.eu/checklist/

[111] GDRP.EU. (20 de 08 de 2024). *News & Updates*. Obtenido de https://gdpr.eu/category/news-updates/

[112] Gellman, B. (2020 de 05 de 2020). *Secret, Surveillance and Snoweden*. Obtenido de https://www.washingtonpost.com/magazine/2020/05/11/2013-edward-snowden-leaked-top-secret-national-security-agency-documents-showing-how-us-was-spying-its-citizens-heres-what-happened-next/

[113] Germain, T. (29 de 04 de 2024). *bbc.com*. Obtenido de https://www.bbc.com/mundo/articles/c3gqnnq055eo#:~:text=TikTok%20parec%C3%ADa%20imparable%2C%20hasta%20que,a%20la%20ma%C3%B1ana%2C%20TikTok%20desapareci%C3%B3.

[114] GMBH, S. M. (14 de 08 de 2024). *Bundesgesetz über den Datenschutz*. Obtenido de https://dsg.ch/

[115] Google. (03 de 09 de 2024). *Geofencing API*. Obtenido de https://developers.google.com/location-context/geofencing?hl=es-419

[116] Google. (26 de 08 de 2024). *Politícas de Privacidad*. Obtenido de https://policies.google.com/privacy?hl=es#footnote-data-controller

[117] Gosuslugi. (04 de 09 de 2024). *Gosuslugi*. Obtenido de https://www.gosuslugi.ru/

[118] Goverment, A. (04 de 09 de 2024). *myGovID*. Obtenido de https://www.mygovid.gov.au/

[119] Government, A. (04 de 09 de 2024). *myGov*. Obtenido de https://my.gov.au/

[120] IBM. (05 de 09 de 2024). *IBM Food Trust*. Obtenido de https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust?utm_content=SRCWW&p1=Search&p4=43700080655818963&p5=e&p9=58700008760843032&gad_source=1&gclid=Cj0KCQjwiuC2BhDSARIsALOVfBISe__POI0w1yAHv5VtYSI4BwAuOh4hUPj5Xo-LXoTKz34U2Y0P9i4aAq_-EALw_

[121] ID4D, W. B. (17 de 10 de 2019). *ID4D Practitioner's Guide*. Obtenido de https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

[122] India, M. o. (15 de 08 de 2024). *Ministry of Electronics & Information Technology Government of India*. Obtenido de https://www.meity.gov.in/content/digital-personal-data-protection-act-2023

[123] infobae. (22 de 06 de 2023). *infobae*. Obtenido de https://www.infobae.com/estados-unidos/2023/06/22/tiktok-admitio-que-almacena-en-china-datos-sensibles-de-usuarios-estadounidenses/

[124] Infomaniaknews. (03 de 09 de 2024). *Infomaniak*. Obtenido de https://news.infomaniak.com/es/cloud-soberano/

[125] Islandia, P. (14 de 08 de 2024). *Lög um persónuvernd og vinnslu persónuupplýsinga*. Obtenido de https://www.althingi.is/lagas/nuna/2018090.html

[126] Japan, P. I. (15 de 08 de 2024). *Personal Information Protection Commission Japan*. Obtenido de https://www.ppc.go.jp/en/legal/

[127] Juan, I. D. (20 de 07 de 2024). *infobae*. Obtenido de https://www.infobae.com/tecno/2024/07/20/suspenden-los-desarrollos-sobre-inteligencia-artificial-de-meta-preocupa-el-uso-de-datos/

[128] Jusbrasil. (13 de 08 de 2024). *Lei Geral de Proteção de Dados Comentada*. Obtenido de https://www.jusbrasil.com.br/legislacao/busca?q=lgpd&utm_source=google&utm_medium=cpc&utm_campaign=lr_dsa_legislacao&utm_term=&utm_content=legislacao&campaign=true&gad_source=1&gclid=Cj0KCQjwiOy1BhDCARIsADGvQnCfaZ-RjagPh6IakLLdmx8hmqUiHm0nBx_zmo5uGvmEB6Gr

[129] Justice, C. D. (13 de 08 de 2024). *CLOUD Act Resources*. Obtenido de https://www.justice.gov/criminal/cloud-act-resources

[130] Justice, S. o. (13 de 08 de 2024). *California Consumer Privacy Act (CCPA)*. Obtenido de https://oag.ca.gov/privacy/ccpa

[131] Kong, L. e. (15 de 08 de 2024). *Legislación electrónica de Hong Kong*. Obtenido de https://www.elegislation.gov.hk/hk/cap486

[132] Learn. (07 de 04 de 2023). *Teams para Administración Pública*. Obtenido de https://learn.microsoft.com/es-es/microsoftteams/expand-teams-across-your-org/teams-for-government-landing-page

[133] Learn, M. (26 de 08 de 2024). *Cumplimiento de Microsoft*. Obtenido de https://learn.microsoft.com/es-es/compliance/

[134] Legal, C. P. (15 de 08 de 2024). *Consulta Plus Soporte Legal*. Obtenido de https://www.consultant.ru/document/cons_doc_LAW_165838/

[135] Malls, A. &. (14 de 03 de 2024). *El auge de los centros de datos en Brasil*. Obtenido de https://america-retail.com/paises/brasil/el-auge-de-los-centros-de-datos-en-brasil/

[136] México, G. d. (13 de 08 de 2024). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Obtenido de https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[137] MIDATA. (05 de 09 de 2024). *My Data – Our Health*. Obtenido de https://www.midata.coop/en/home/

[138] Ministerio de la Presidencia, J. y.-G. (13 de 08 de 2024). *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*. Obtenido de https://www.boe.es/eli/es/lo/2018/12/05/3/con

[139] Moneda, S. E. (05 de 09 de 2024). *Certificado Electrónico de Ciudadano*. Obtenido de https://www.sede.fnmt.gob.es/certificados/persona-fisica

[140] Mundo, E. (21 de 01 de 2019). *El Mundo*. Obtenido de https://www.elmundo.es/economia/empresas/2019/01/21/5c45e159fc6c8305148b4693.html

[141] NextCloud. (03 de 09 de 2024). *NextCloud*. Obtenido de https://nextcloud.com/

[142] OPENGOV. (04 de 09 de 2024). *About*. Obtenido de https://opengov.com/about/

[143] OVHcloud. (05 de 09 de 2024). *Hosting y dominios*. Obtenido de https://www.ovhcloud.com/es-es/web-hosting/web-hosting-france/

[144] OwnCLoud. (03 de 09 de 2024). *OwnCLoud*. Obtenido de https://owncloud.com/

[145] Platform, I. A. (05 de 09 de 2024). *Healthcare Cybersecurity*. Obtenido de https://www.ignyteplatform.com/healthcare-cybersecurity/

[146] Pública, M. p. (05 de 09 de 2024). *Avance Digital*. Obtenido de https://avancedigital.mineco.gob.es/5G/Paginas/Actuaciones-5G-Europa.aspx

[147] Pucihar, A., Kljajic Borstnar, M., Bons, R., Ongena, G., Heikkila, M., & Vidmar, D. (2023). *36th Bled eConference: "Digital Economy and Society: The Balancing Act for Digital Innovation in Times of Instability, BLED 2023 - Proceedings".* Bled: University of Maribor Press.

[148] Radar. (03 de 09 de 2024). *Radar*. Obtenido de https://radar.com/

[149] Region, N. o. (01 de 20 de 2024). *Sinnet Customer Agreement for Amazon Web Services*. Obtenido de https://www.amazonaws.cn/en/agreement/beijing/

[150] Scassa, T. (2019). Data Protection in the Internet: Canada. En D. M. Casimiro, *Data Protection and the Internet* (págs. 55-76). Otawa, Canada: Springer.

[151] SNDS, S. N. (05 de 09 de 2024). *Qu'est-ce que le SNDS?* Obtenido de https://www.snds.gouv.fr/SNDS/Qu-est-ce-que-le-SNDS

[152] Supervisor, E. D. (07 de 09 de 2024). *Annual Reports*. Obtenido de https://www.edps.europa.eu/annual-reports_en

[153] THALES. (05 de 09 de 2024). *Protegrity*. Obtenido de https://cpl.thalesgroup.com/partners/protegrity

[154] THALES. (05 de 09 de 2024). *Vormetric Data Security Platform*. Obtenido de https://cpl.thalesgroup.com/encryption/vormetric-data-security-platform

[155] TrustArc. (05 de 09 de 2024). *International Data Transfers*. Obtenido de https://trustarc.com/solutions/international-data-transfers/

[156] Turco, P. D. (15 de 08 de 2024). *Personal Data Protection Authority*. Obtenido de https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

[157] Uber. (17 de 07 de 2024). *Aviso de privacidad de Uber*. Obtenido de https://www.uber.com/legal/es/document/?name=privacy-notice&country=india&lang=en#kix.mqhz0aioaflf

[158] WEBEX. (05 de 09 de 2024). *Government*. Obtenido de https://www.webex.com/es/industries/government.html

[159] Website, A. S. (04 de 09 de 2024). *singpass*. Obtenido de https://www.singpass.gov.sg/main

Anexo 1: Leyes en países sobre Protección de Datos

Continente	País	Leyes	Características destacadas	Influencias internacionales
América Norte	Estados Unidos	No existe una ley federal unificada de protección de datos	Sectorialización de las leyes (HIPAA, GLBA, CCPA, etc.), enfoque en la autorregulación de las empresas.	OCDE
América Norte	Canadá	Ley de Protección de la Información Personal y los Documentos Electrónicos (PIPEDA)	Ley federal que cubre el sector privado, principios similares al RGPD, autoridad de control independiente.	OCDE, RGPD
América Norte	México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)	Ley integral, enfocada en los derechos de los individuos, autoridad de control independiente.	OCDE, RGPD
América del Sur	Argentina	Ley N.ª 25.326 Ley de Protección de Datos Personales	Enfoque en el consentimiento informado, autoridad de control, adaptación al RGPD.	RGPD, OCDE
América del Sur	Brasil	Ley General de Protección de Datos (LGPD)	Inspirada en el RGPD, derechos amplios para los titulares de datos, sanciones severas.	RGPD, OCDE
América del Sur	Chile	Protección de la Vida Privada (Ley N.º 19.628 de 1999)	Protección integral de los datos personales, autoridad de control, adaptación al RGPD.	RGPD, OCDE
América del Sur	Colombia	Ley 1581 Ley de Protección de Datos Personales de 2012	Enfoque en la protección de la información personal, principios de legalidad, finalidad, calidad, etc.	RGPD, OCDE
América del Sur	Perú	Ley N.º 29733 Ley de Protección de Datos Personales	Protección de los datos personales, derechos de los titulares, autoridad de control.	RGPD, OCDE

América del Sur	Uruguay	Ley N.º 18.331 Ley de Protección de Datos Personales	Protección de los datos personales, principios de legalidad, finalidad, calidad, etc.	RGPD, OCDE
América del Sur	Ecuador	Ley Orgánica de Protección de Datos Personales (LOPD) 2021	Impone restricciones sobre la transferencia internacional de datos, solo permitida cuando se garantice un nivel adecuado de protección.	Propia
América del Sur	Paraguay	Ley de Protección de Datos Crediticios Personales o Ley de Datos Crediticios.	Aunque no obliga la localización de datos, establece restricciones para la transferencia internacional de datos.	Propia
América del Sur	Bolivia	Constitución Política del Estado (Art. 130 y 131)	No tiene una ley específica de protección de datos, pero la constitución protege la privacidad y el uso de los datos personales.	Propia
América Central	Barbados	La Ley de Protección de Datos de 2019	La Ley, que protege la privacidad de las personas, regula la recopilación, conservación, procesamiento, uso y difusión de datos personales.	Propia
América Central	Bahamas	La Ley de Protección de Datos (Privacidad de la Información Personal) de 2007	Otorga a los ciudadanos de las Bahamas el derecho de acceso, rectificación y eliminación, y el derecho a prohibir cualquier forma de procesamiento de datos con fines de marketing directo.	Propia
América Central	Costa Rica	Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales	Adaptación a estándares internacionales, enfoque en los derechos de los individuos, Superintendencia de Telecomunicaciones (Sutel).	RGPD, OCDE

América Central	Jamaica	Ley de Protección de Datos de Jamaica N.º 7	La Ley define las funciones y responsabilidades de un responsable del tratamiento de datos y otorga derechos sobre los datos a las personas que hayan fallecido hace menos de 30 años.	Propia
América Central	Islas Vírgenes Británicas	Ley de Protección de Datos de 2021	Cuenta con un conjunto adecuado de medidas de privacidad de datos equivalentes a los estándares del Reino Unido y la UE, ya que una multitud de empresas de la UE y el Reino Unido dependen del territorio para realizar operaciones financieras sin problemas.	Propia
América Central	Panamá	Ley general de protección de datos, Autoridad Nacional para la Transparencia y el Acceso a la Información (ANTAI)	Ley general de protección de datos, Autoridad Nacional para la Transparencia y el Acceso a la Información (ANTAI).	OCDE
América Central	Venezuela	Ley de Protección de Datos Personales (2021)	Nueva ley que establece principios de protección de datos personales y regula la transferencia internacional de datos.	Propia
América Central	Honduras	Ley de Protección de Datos Personales (2019)	Regula la protección de datos personales y limita la transferencia de datos a países que no ofrezcan protecciones adecuadas.	Propia
América Central	El Salvador	Ley de Protección de Datos Personales (2021)	Establece reglas sobre la protección y transferencia de datos personales a nivel internacional.	Propia

América Central	República Dominicana	Ley de Protección de Datos Personales (2022)	Nueva ley que regula la protección de datos y limita la transferencia a países sin niveles adecuados de protección.	Propia
América Central	Guatemala	Ley de Protección Integral de Datos Personales (2021)	Regula el manejo de datos personales y su transferencia a países que ofrezcan protección adecuada.	Propia
América Central	Nicaragua	Ley de Protección de Datos Personales (2020)	Regula la protección de datos y establece criterios para la transferencia internacional de datos personales.	Propia
América Central	Puerto Rico	Proyecto de Ley de la Cámara 655 y Proyecto de Ley del Senado 882	tiene como objetivo establecer la "Ley de privacidad de la información electrónica" para proteger el derecho de las personas a la privacidad sobre la información almacenada en un dispositivo electrónico o transmitida a un proveedor de servicios informáticos remoto	Propia
Europa del Norte	Dinamarca	Person data forordningen (PDFO)	Adaptación del RGPD, enfoque en la transparencia y el consentimiento informado.	RGPD, OCDE
Europa del Norte	Finlandia	Laki henkilötietojen suojasta (1050/2018)	Basada en el RGPD, énfasis en los derechos de los individuos y la supervisión independiente.	RGPD, OCDE
Europa del Norte	Islandia	Lög um persónuvernd (nr. 90/2018)	Implementación del RGPD, autoridad de control independiente, enfoque en la protección de la privacidad.	RGPD, OCDE
Europa del Norte	Noruega	Personopplysningsloven (PUL)	Adaptación del RGPD, énfasis en la protección de la privacidad y los derechos de los individuos.	RGPD, OCDE

Europa Norte	Suecia	Dataskyddsförordningen (GDPR)	Implementación directa del RGPD, autoridad de control activa, enfoque en la transparencia.	RGPD, OCDE
Europa Norte	Rusia	Ley Federal N.º 152-FZ "Sobre la información, las tecnologías de la información y la protección de la información", Ley Federal No. 242-FZ Ley soberanía de datos	Tiene como referencia el convenio 108 del Consejo de Europa y prácticas comunes de otros países.	Convenios 108
Europa Norte	Letonia	Reglamento General de Protección de Datos (GDPR)	El GDPR está en vigencia y regulado por la Inspección de Datos del Estado de Letonia.	RGPD, OCDE
Europa Norte	Estonia	Reglamento General de Protección de Datos (GDPR)	Implementa el GDPR bajo la Inspección de Protección de Datos de Estonia.	RGPD, OCDE
Europa Norte	Lituania	Reglamento General de Protección de Datos (GDPR)	El GDPR es aplicado bajo la supervisión de la Inspección Estatal de Protección de Datos.	RGPD, OCDE
Europa Sur	España	Reglamento General de Protección de Datos (GDPR) y Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)	Adaptación del RGPD, Agencia Española de Protección de Datos (AEPD), enfoque en los derechos digitales.	RGPD, OCDE
Europa Sur	Portugal	Regulamento Geral de Proteção de Dados (RGPD)	Implementación directa del RGPD, Comisión Nacional de Proteção de Dados (CNPD).	RGPD, OCDE
Europa Sur	Italia	Codice in materia di protezione dei dati personali (D.lgs. 196/2003, modificato dal D.lgs. 101/2018)	Adaptación al RGPD, Garante per la protezione dei dati personali.	RGPD, OCDE
Europa Sur	Grecia	Νόμος 4624/2019	Implementación del RGPD, Autoridad Griega de Protección de Datos Personales.	RGPD, OCDE
Europa Sur	Malta	Data Protection Act (2018)	Implementación del RGPD, Oficina del Comisionado de Información y Protección de Datos.	RGPD, OCDE

Europa Sur	Suiza	LFPD (Ley Federal Suiza de Protección de Datos) (2020)	La ley revisada amplía la definición de datos personales sensibles al incluir datos genéticos y biométricos.	Propia
Europa Este	Polonia	Ustawa o ochronie danych osobowych (UODO)	Adaptación del RGPD, enfoque en los derechos de los individuos, Presidente del Órgano de Protección de Datos Personales.	RGPD, OCDE
Europa Este	República Checa	Zákon o ochraně osobních údajů (ZOÚ)	Implementación del RGPD, Úřad pro ochranu osobních údajů (ÚOOÚ).	RGPD, OCDE
Europa Este	Austria	Datenschutzgesetz (DSG) y RGPD	Ley integral, fuerte protección de los derechos individuales, Autoridad de Protección de Datos.	RGPD, OCDE
Europa Este	Hungría	Törvény a természetes személyeknek a személyes adatok kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról (2011. évi CXIX. törvény)	Adaptación del RGPD, Nemzeti Adatvédelmi Biztos.	RGPD, OCDE
Europa Este	Rumanía	Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date	Adaptación al RGPD, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).	RGPD, OCDE
Europa Este	Eslovaquia	Zákon o ochrane osobných údajov č. 18/2018 Z. z.	Implementación del RGPD, Úrad na ochranu osobných údajov (ÚOOÚ).	RGPD, OCDE
Europa Oeste	Alemania	Bundesdatenschutzgesetz (BDSG)	Adaptación del RGPD, enfoque en la privacidad desde su origen, fuerte autoridad de control (BfDI).	RGPD, OCDE
Europa Oeste	Francia	Loi Informatique et Libertés	Adaptación del RGPD, Comisión Nacional de Informatique et Libertés (CNIL),	RGPD, OCDE

			enfoque en la transparencia y la rendición de cuentas.	
Europa Oeste	Reino Unido	UK GDPR	Implementación del RGPD antes del Brexit, Information Commissioner's Office (ICO).	RGPD, OCDE
Europa Oeste	Irlanda	General Data Protection Regulation (GDPR)	Implementación directa del RGPD, Data Protection Commission (DPC).	RGPD, OCDE
Europa Oeste	Bélgica	Wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens	Adaptación del RGPD, Autoriteit voor de Bescherming van Persoonsgegevens (AP).	RGPD, OCDE
Europa Oeste	Países Bajos	Algemene verordening gegevensbescherming (AVG)	Implementación directa del RGPD, Autoriteit Persoonsgegevens (AP).	RGPD, OCDE
Europa Oeste	Croacia	Reglamento General de Protección de Datos (GDPR)	Aplica el GDPR, supervisado por la Agencia Croata para la Protección de Datos Personales (AZOP).	RGPD, OCDE
Europa Oeste	Rumanía	Reglamento General de Protección de Datos (GDPR)	El GDPR se implementa plenamente, bajo la supervisión de la Autoridad Nacional para la Supervisión del Procesamiento de Datos Personales.	RGPD, OCDE
Europa Oeste	Bulgaria	Reglamento General de Protección de Datos (GDPR)	Implementa el GDPR, regulado por la Comisión de Protección de Datos.	RGPD, OCDE
Europa Oeste	Eslovenia	Reglamento General de Protección de Datos (GDPR)	El GDPR es supervisado por la Comisión de Información de Eslovenia.	RGPD, OCDE
Europa Oeste	Chipre	Reglamento General de Protección de Datos (GDPR)	Aplica el GDPR y está supervisado por la Oficina del Comisionado para la Protección de Datos Personales.	RGPD, OCDE
Europa Oeste	Luxemburgo	Règlement général sur la protection des données (RGPD)	Implementación directa del RGPD, Commission nationale	RGPD, OCDE

			pour la protection des données (CNPD).	
Europa, Oriente Medio y África	Kazajstán	Ley de la República de Kazajstán N.º 94-V	El Ministerio de Desarrollo Digital, Innovaciones y Aeroespacial publicó un proyecto de modificaciones que se realizarían a esta ley para introducir requisitos de notificación, la prohibición del uso de datos personales sin el consentimiento del usuario, el derecho de los usuarios al borrado, así como una serie de otras medidas de seguridad y obligaciones para los controladores y procesadores de datos.	Propia
Europa, Oriente Medio y África	Tayikistán	Ley de Protección de Datos Personales	Es la principal legislación que otorga a los ciudadanos tayikos el acceso a los derechos de los datos, al tiempo que impone obligaciones y requisitos a las organizaciones en lo que respecta a los datos personales de los tayikos en línea.	Propia
Europa, Oriente Medio y África	Eslovaquia	Ley de Protección de Datos de Eslovaquia	armoniza e implementa el RGPD en el país.	Propia
Europa, Oriente Medio y África	Serbia	Ley de Protección de Datos Personales	La Ley de Protección de Datos Personales es bastante similar al RGPD.	Propia
Europa, Oriente Medio y África	Montenegro	Ley de Protección de Datos Personales	Es una de las pocas leyes de protección de datos en Europa que preceden al RGPD.	Propia
Europa, Oriente Medio y África	Mauricio	Ley de Protección de Datos de 2017	Dado que Mauricio es signatario del Acuerdo de Asociación Económica (AAE) provisional	Propia

			con la UE, la AAE de 2017 es una forma eficaz de alinear su marco de protección de datos con el de la UE.	
Europa, Oriente Medio y África	Malta	Ley de Protección de Datos de 2018	El Comisionado de Información y Protección de Datos es la principal autoridad supervisora que hace cumplir la Ley de Protección de Datos y también representa a Malta en el Comité Europeo de Protección de Datos.	Propia
Europa, Oriente Medio y África	Georgia	La Ley de Georgia sobre Protección de Datos Personales (N5669-RS, 28/12/2011)	La ley tiene como objetivo proteger el derecho a la privacidad de los georgianos y garantizar que cualquier organización que procese sus datos tenga las medidas necesarias para garantizar la protección de este derecho.	Propia
Europa, Oriente Medio y África	Bélgica	Ley de Protección de Datos de 2018	s la principal ley de protección de datos en Bélgica que prevé la aplicación de las disposiciones del RGPD que requieren más aclaraciones, requisitos o derogaciones.	RGPD
Europa, Oriente Medio y África	Azerbaiyán	La Ley de Información Personal, aprobada en 2010,	es la principal regulación de protección de datos en el país. La ley introdujo dos categorías separadas de todos los datos: personales y sensibles.	Propia
Europa, Oriente Medio y África	Armenia	La Ley Nº HO-49-N del 18 de mayo de 2015 sobre la Protección de Datos Personales es la principal normativa de protección de datos en el país.	Regula varios aspectos relacionados con la privacidad de los datos de los ciudadanos armenios, así como las responsabilidades de todas las	Propia

			autoridades y privadas que recopilan, procesan, almacenan, comparten y venden los datos personales de los armenios.	
Europa, Oriente Medio y África	Albania	La Ley n.º 9887 sobre la protección de datos personales en Albania precede al RGPD.	La autoridad independiente de Albania, la Oficina del Comisionado de Información y Protección de Datos (IDP), es responsable de hacer cumplir la Ley n.º 9887 en el país y garantizar la protección de los datos personales.	RGPD
Europa, Oriente Medio y África	Ucrania	Ley de protección de datos personales	La Ley de 1 de junio de 2010 N.º 2297-VI sobre Protección de Datos Personales, más conocida como la Ley de Protección de Datos Personales, es la principal ley de protección de datos en Ucrania.	Propia
Europa, Oriente Medio y África	Jordania	Ley de protección de datos personales de 2021	En diciembre de 2021, el Consejo de Ministros de Jordania aprobó el proyecto de ley de protección de datos personales (PDPL).	Propia
Europa, Oriente Medio y África	Omán	Ley de Protección de Datos Personales de Omán	La LPPD, cuyo cumplimiento está a cargo del Ministerio de Transportes, Comunicaciones y Tecnologías de la Información (MTCIT), otorgará a los residentes omaníes una privacidad de datos equivalente a la del resto del mundo.	Propia
Europa, Oriente Medio y África	Eswatini	Ley de Protección de Datos de Eswatini	La Comisión de Comunicaciones de Eswatini publicó la Ley de Protección de	Propia

			Datos N.º 5 de 2022 y anunció simultáneamente su aplicación inmediata.	
Europa, Oriente Medio y África	Bielorrusia	Ley de Protección de Datos Personales de Belarús N.º 99-Z	Se trata de la primera ley de este tipo en Bielorrusia y su finalidad es aplicar las disposiciones del Protocolo sobre Tecnologías de la Información y la Comunicación e Interacción Informativa en la Unión Económica Euroasiática.	Propia
Europa, Oriente Medio y África	Andorra	Ley de Protección de Datos Personales de Andorra	La ley se aplica al tratamiento total o parcialmente automatizado y no automatizado de datos personales por parte de personas o empresas ubicadas en Andorra.	Propia
Europa, Oriente Medio y África	Bahréin	Ley de Protección de Datos Personales de Bahréin (PDPL)	La PDPL reconoce los derechos de las personas a tener un mayor control sobre sus datos personales y las necesidades de las organizaciones de recopilar, usar o divulgar datos personales con fines legítimos.	Propia
Europa, Oriente Medio y África	Botsuana	Ley de Protección de Datos de Botsuana N.º 32	La ley contiene todas las disposiciones importantes en materia de datos necesarios para proteger adecuadamente los derechos de los ciudadanos de Botsuana en línea sobre sus datos.	Propia
Europa, Oriente Medio y África	Mónaco	Ley n.º 1.165 sobre la protección de datos personales	Es la principal ley de protección de datos en Mónaco, mientras que la Comisión de Control de Datos Personales (CCIN) es la autoridad reguladora de la	Propia

			protección de datos, también responsable de la aplicación de la Ley de Protección de Datos Personales.	
Europa, Oriente Medio y África	Zimbabue	Ley de Protección de Datos de Zimbabwe	La DPA se centra en la privacidad de los datos, así como en la ciberseguridad y la prevención de los delitos cibernéticos.	Propia
Europa, Oriente Medio y África	Kuwait	Reglamento de protección de datos personales de Kuwait	El DPPR contiene disposiciones esenciales relacionadas con la responsabilidad de las organizaciones hacia sus usuarios y otros aspectos relacionados con el cifrado, los centros de datos y las condiciones de procesamiento de datos.	Propia
África Norte	Marruecos	Ley 18-15 relativa a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal	Adaptación a estándares internacionales, enfoque en los derechos de los individuos, Comisión Nacional de Control de la Protección de Datos Personales.	RGPD, OCDE
África Norte	Túnez	Ley n.º 2018-58 relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales	Adaptación al RGPD, enfoque en la transparencia y la rendición de cuentas, Autoridad de Protección de Datos Personales.	RGPD, OCDE
África Norte	Argelia	Ley n.º 17-19 relativa a la protección de las personas físicas con respecto al tratamiento de los datos de carácter personal	Adaptación a estándares internacionales, enfoque en la protección de la privacidad, Comisión Nacional de Control de la Protección de Datos Personales.	RGPD, OCDE

África Norte	Egipto	Ley 152 de 2020 sobre la protección de datos personales	Ley reciente, adapta estándares internacionales, Autoridad de Protección de Datos Personales.	RGPD, OCDE
África Sur	Sudáfrica	Protección of Personal Information Act (POPIA)	Ley integral de protección de datos, enfoque en los derechos de los individuos, Information Regulator.	RGPD, OCDE
África Sur	Namibia	Protection of Personal Information Act	Adaptación a estándares internacionales, enfoque en la transparencia y la rendición de cuentas, Office of the Commissioner for Privacy.	RGPD, OCDE
África Sur	Mauricio	Ley de Protección de Datos (2017)	Regula la transferencia de datos personales al extranjero, permitiéndola solo si el país de destino garantiza la protección adecuada.	RGPD, OCDE
África Sur	Malawi	Ley de Protección de Datos Personales (2021)	Regula la transferencia internacional de datos, solo permitiendo su traslado a países con garantías de protección.	RGPD, OCDE
África Occidental	Nigeria	Nigeria Data Protection Regulation (NDPR)	Ley integral de protección de datos, enfoque en los derechos de los individuos, National Data Protection Commission (NDPC).	RGPD, OCDE
África Occidental	Ghana	Data Protection Act, 2012 (Act 843)	Ley pionera en la región, enfoque en la protección de la privacidad, Data Protection Commission.	OCDE
África Occidental	Senegal	Loi n.º 2019-03 du 23 janvier 2019 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	Adaptación a estándares internacionales, enfoque en los derechos de los individuos, Commission Nationale de Protection des Données Personnelles.	RGPD, OCDE

África Occidental	Costa de Marfil	Loi n° 2019-944 du 27 décembre 2019 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	Ley reciente, adapta estándares internacionales, Autorité de Protection des Données à Caractère Personnel.	RGPD, OCDE
África Occidental	Benín	Loi n° 2019-022 du 12 juin 2019 portant protection des personnes physiques à l'égard du traitement des données à caractère personnel	Ley reciente, adapta estándares internacionales, Autorité de Protection des Données à Caractère Personnel.	RGPD, OCDE
África Occidental	Cabo Verde	Ley de Protección de Datos Personales (2001)	Regula la transferencia de datos internacionales, permitiéndola solo a países con niveles adecuados de protección.	Propia
África Austral	Sudáfrica	Protección of Personal Information Act (POPIA)	Ley integral de protección de datos, enfoque en los derechos de los individuos, Information Regulator.	RGPD, OCDE
África Austral	Namibia	Protection of Personal Information Act	Adaptación a estándares internacionales, enfoque en la transparencia y la rendición de cuentas, Office of the Commissioner for Privacy.	RGPD, OCDE
África Austral	Botswana	Personal Data Protection Act	Ley reciente, adapta estándares internacionales, Independent Data Protection Authority.	RGPD, OCDE
África Oriental	Kenia	Data Protection Act, 2019	Ley reciente, adapta estándares internacionales, Data Protection Authority.	RGPD, OCDE
África Oriental	Tanzania	Electronic Transactions Act, 2016	Aunque no es una ley específica de protección de datos, incluye disposiciones sobre la protección de datos.	OCDE
África Oriental	Uganda	Data Protection and Privacy Act, 2019	Ley reciente, adapta estándares internacionales, Data Protection and Privacy Commissioner.	RGPD, OCDE

África Oriental	Ruanda	Law No. 59/2019 of 24/08/2019 on the Protection of Personal Data	Ley reciente, adapta estándares internacionales, Rwanda Utilities Regulatory Authority (RURA).	RGPD, OCDE
África Oriental	Seychelles	Ley de Protección de Datos (2003)	Establece regulaciones similares a las del GDPR, limitando la transferencia internacional de datos personales.	RGPD, OCDE
África Oriental	Etiopía	Ley de Protección de Datos Personales (2020)	Prohíbe la transferencia de datos personales fuera del país, salvo que se garantice una protección adecuada.	RGPD, OCDE
África Centro	Zambia	Ley de Protección de Datos Personales (2021)	Similar al GDPR, regula la transferencia internacional de datos bajo condiciones que aseguren la protección adecuada.	RGPD, OCDE
Asia Oriental	China	Ley de Protección de la Información Personal (PIPL) y Ley de Seguridad de Datos de China (DSL)	La PIPL es sobre la protección de datos y la DSL sobre el procesamiento de datos. Leyes integrales, enfoque en la seguridad nacional, Comisión Nacional de Desarrollo y Reforma.	RGPD, pero con fuertes matices locales
Asia-Pacífico	Uzbekistán	Ley de Datos Personales	Esta ley designa al Gabinete de Ministros de la República de Uzbekistán (el “Gabinete de Ministros”) y al Centro Estatal de Personalización dependiente del Gabinete de Ministros (el “Centro Estatal de Personalización”) como los principales órganos reguladores en materia de protección de datos personales.	Propia

Asia-Pacífico	Mongolia	Ley de Protección de Datos Personales	El Gran Khural Estatal de Mongolia, también conocido como el Parlamento de Mongolia, aprobó la Ley de Protección de la Información Personal en diciembre de 2021.	Propia
Asia-Pacífico	Birmania	Myanmar: Enmiendas a la Ley de protección de la privacidad y la seguridad de los ciudadanos (2017) y a la Ley de transacciones electrónicas (2004)	Ley de Protección de la Privacidad y Seguridad de los Ciudadanos (2017), más conocida simplemente como la "Ley de Privacidad", parece ser la principal normativa de protección de datos en Myanmar. En febrero de 2021 se añadieron varias modificaciones a sus disposiciones.	Propia
Asia-Pacífico	Brunéi Darussalam	Proyecto de orden sobre protección de datos personales	En mayo de 2021, la Autoridad de la Industria de Tecnologías de la Información y las Comunicaciones de Brunei Darussalam (AITI) solicitó una consulta pública y respuestas sobre su propuesta de Orden de Protección de Datos Personales.	Propia
Asia-Pacífico	Sri Lanka	Ley de Protección de Datos Personales de Sri Lanka	La legislación cubre todas las bases importantes al otorgar a los ciudadanos de Sri Lanka derechos como titulares de los datos, al tiempo que impone varias obligaciones relacionadas con los datos a las organizaciones que procesan los datos de los usuarios dentro del país. También se pueden	Propia

			imponer sanciones estrictas a las organizaciones que no cumplan con la PDPA.	
Asia-Pacífico	Hong Kong	Ordenanza sobre privacidad y datos personales de Hong Kong (PDPO)	La PDPO sirve como el principal marco legislativo en Hong Kong destinado a salvaguardar la privacidad de los datos personales de las personas y, al mismo tiempo, rige las prácticas de recopilación, almacenamiento, procesamiento y divulgación de datos por parte de las organizaciones del sector público y privado, independientemente del lugar de procesamiento, siempre que los datos sean gestionados por un usuario de datos con sede en Hong Kong.	Propia
Asia Oriental	Japón	Ley de Protección de Información Personal (APPI)	Enfoque en la privacidad, Agencia de Protección de la Información Personal.	OCDE, principios de privacidad
Asia Oriental	Corea del Sur	Ley de Protección de Información Personal (PIPL)	Enfoque en la privacidad, Comisión de Protección de Información Personal.	OCDE, principios de privacidad
Asia Oriental	Taiwán	Ley de Protección de Datos Personales (PDPA)	Enfoque en la privacidad, Comisión de Protección de Información Personal.	RGPD, OCDE
Asia Oriental	Mongolia	Ley de Protección de Datos Personales	Enfoque en la privacidad, Agencia Nacional de Seguridad de la Información.	RGPD, OCDE
Sudeste Asiático	Vietnam	Decreto de Seguridad Cibernética (2018)	Obliga a las empresas a almacenar datos personales y críticos dentro del país, con fuertes restricciones en la	RGPD, OCDE

			transferencia de datos fuera de Vietnam.	
Asia Meridional	India	Ley de Protección de Datos Personales (PDPA)	Ley reciente, enfoque en la privacidad, Autoridad de Protección de Datos de India.	RGPD, OCDE
Asia Meridional	Sri Lanka	Proyecto de Ley de Protección de Datos Personales (2022)	Regula la protección de datos y limita la transferencia a países con niveles adecuados de protección.	RGPD, OCDE
Asia Meridional	Nepal	Ley de Privacidad de Datos (2018)	Establece la protección de datos personales y regula su transferencia fuera del país bajo condiciones estrictas.	RGPD, OCDE
Asia Meridional	Turquía	Ley de Protección de Datos Personales de Turquía (LPPD)	Similar al GDPR, regula la transferencia internacional de datos solo a países que proporcionen un nivel adecuado de protección.	RGPD, OCDE
Sudeste Asiático	Singapur	Personal Data Protection Act (PDPA)	Ley integral, enfoque en la privacidad, Personal Data Protection Commission (PDPC).	RGPD, OCDE
Sudeste Asiático	Indonesia	Ley de Protección de Datos Personales (PDPL)	Ley reciente, adapta estándares internacionales, Comisión de Protección de Datos Personales.	RGPD, OCDE
Sudeste Asiático	Malasia	Ley de Protección de Datos Personales (PDPA)	Ley integral, enfoque en la privacidad, Departamento de Protección de Datos Personales.	RGPD, OCDE
Sudeste Asiático	Filipinas	Ley de Privacidad de Datos (DPA)	Ley reciente, adapta estándares internacionales, Comisión Nacional de Privacidad.	RGPD, OCDE
Sudeste Asiático	Bangladés	Proyecto de Ley de Protección de Datos Personales (2022)	Similar al GDPR, regula la transferencia de datos solo a países que garantizan una protección adecuada.	RGPD, OCDE

Sudeste Asiático	Tailandia	Ley de Protección de Datos Personales (PDPA)	Ley reciente, adapta estándares internacionales, Comisión de Protección de Datos Personales.	RGPD, OCDE
Asia Occidental	Arabia Saudita	Ley de Protección de Datos Personales (PDPL) y Ley de comercio electrónico de Arabia Saudita (ECL)	Ley reciente, adapta estándares internacionales, Autoridad de Protección de Datos.	RGPD, OCDE
Asia Occidental	Emiratos Árabes Unidos	La Ley de Protección de Datos del Centro Financiero Internacional de Dubái (DIFC) de 2020	La Ley de Protección de Datos del DIFC establece obligaciones para las organizaciones en relación con la recopilación, divulgación y procesamiento de datos personales en el DIFC, una zona económica especial de Dubái.	RGPD, OCDE
Asia Occidental	Bahréin	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Comité de Protección de Datos.	RGPD, OCDE
Asia Occidental	Qatar	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Autoridad de Protección de Datos.	RGPD, OCDE
Asia Occidental	Omán	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Autoridad de Protección de Datos.	RGPD, OCDE
Asia Occidental	Kuwait	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Autoridad de Protección de Datos.	RGPD, OCDE
Asia Occidental	Jordania	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Comisión de Protección de Datos.	RGPD, OCDE
Asia Occidental	Israel	Ley de Protección de la Privacidad	Ley integral, enfoque en la privacidad, Autoridad de Protección de la Privacidad.	OCDE
Asia Occidental	Irán	Ley de Ciberseguridad	Aunque no es una ley específica de protección de datos, incluye	RGPD, OCDE

			disposiciones sobre la protección de datos.	
Asia Central	Kazajistán	Ley de Protección de Datos Personales	Ley integral, adapta estándares internacionales, Comité Nacional de Seguridad de Estado.	RGPD, OCDE
Asia Central	Kirguistán	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Agencia Nacional de Seguridad de la Información.	RGPD, OCDE
Asia Central	Tayikistán	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Agencia Nacional de Seguridad de la Información.	RGPD, OCDE
Asia Central	Uzbekistán	Ley de Protección de Datos Personales	Ley reciente, adapta estándares internacionales, Agencia Nacional de Seguridad de la Información.	RGPD, OCDE
Oceanía	Nueva Zelanda	Ley de Privacidad de Nueva Zelanda (NZPA) de 2020	La NZPA introduce requisitos obligatorios de notificación de infracciones, incluida la obligación de notificar incluso aquellas infracciones de privacidad causadas por un tercero subcontratado, además de otras obligaciones de protección de datos.	OCDE, algunos elementos del RGPD
Oceanía	Fiyi	Personal Data Protection Act 2014	Ley reciente, adapta estándares internacionales, Oficina del Comisionado de Información.	RGPD, OCDE
Oceanía	Islas Salomón	Privacy Act 2019, Ley de	Ley reciente, adapta estándares internacionales, Comisión de Privacidad.	RGPD, OCDE
Oceanía	Papúa Nueva Guinea	Privacy Act 1998	Ley más antigua de la región, enfoque en los sectores financieros y de	OCDE

			telecomunicaciones, Oficina del Comisionado de Privacidad.	
Oceanía	Vanuatu	Personal Data Protection Act 2013	Ley reciente, adapta estándares internacionales, Oficina del Comisionado de Privacidad.	RGPD, OCDE
Oceanía	Australia	Privacy Act 1988	Protección de la información personal	RGPD, OCDE
Oceanía	Samoa	Ley de Protección de Datos Personales (2021)	Regula el uso de datos personales y permite su transferencia internacional bajo acuerdos que aseguren su protección.	

Elaboración propia

Anexo 2: Reporte de FTC

Federal Trade Commision (FTC): Protección de la privacidad y la seguridad de los datos de los estadounidenses [84].

Orden de metaconsentimiento:

1. La FTC propuso cambios a la orden de privacidad de 2020 de la agencia con Facebook, Inc., después de alegar que la compañía no cumplió plenamente con la orden, engañó a los padres sobre su capacidad para controlar con quién se comunicaban sus hijos a través de su aplicación Messenger Kids y tergiversó el acceso que brindaba a algunos desarrolladores de aplicaciones a datos privados de los usuarios. Como parte de los cambios propuestos, Meta, que cambió su nombre de Facebook en octubre de 2021, tendría prohibido beneficiarse de los datos que recopila, incluso a través de sus productos de realidad virtual, de usuarios menores de 18 años. También estaría sujeto a otras limitaciones ampliadas, incluido el uso de tecnología de reconocimiento facial, y la obligación de proporcionar protecciones adicionales para los usuarios.

Órdenes de la Ley de Protección de la Privacidad Infantil en Línea:

1. La FTC obtuvo acuerdos que requieren que Epic Games, Inc., creador del popular videojuego Fortnite, pago un total de $520 millones en compensación por las acusaciones de que la compañía violó la Ley de Protección de la Privacidad Infantil en Línea (COPPA) e implementó trucos de diseño, conocidos como patrones oscuros, para engañar a millones de jugadores para que realizaran compras no intencionadas. La acción de la FTC contra Epic implica dos acuerdos separados que batieron récords. Como parte de una orden judicial federal propuesta presentada por el DOJ en nombre de la FTC, Epic pagará una multa monetaria de 275 millones de dólares por violar la regla COPPA, que es la multa más grande jamás obtenida por violar una regla de la FTC. Además, en una disposición única en su tipo, Epic deberá adoptar configuraciones predeterminadas de privacidad sólidas para niños y adolescentes, garantizando que las comunicaciones de voz y texto estén desactivadas de forma predeterminada. Según una orden administrativa separada, Epic pagará 245 millones de dólares para reembolsar a los consumidores por sus

patrones oscuros y prácticas de facturación, que es el monto de reembolso más grande de la FTC en un caso de juegos.

2. Según la denuncia presentada por el DOJ en nombre de la FTC, Amazon impidió a los padres ejercer sus derechos de eliminación según la regla COPPA, conservó datos confidenciales de voz y geolocalización durante años y los utilizó para sus propios fines, al tiempo que ponía los datos en riesgo de daño por acceso innecesario.
3. Microsoft Corporation pagará 20 millones de dólares para resolver los cargos de la FTC por violar la COPPA al recopilar información personal de niños que se registraron en su sistema de juegos Xbox sin notificar a sus padres ni obtener el consentimiento de sus padres, y al retener ilegalmente información personal de los niños. Como parte de una orden propuesta presentada por el DOJ en nombre de la FTC, se requerirá que Microsoft tome varias medidas para reforzar la protección de la privacidad de los usuarios infantiles de su sistema Xbox. Por ejemplo, la orden ampliará las protecciones COPPA a los editores de juegos externos con quienes Microsoft comparte datos de niños. Además, la orden deja claro que los avatares generados a partir de la imagen de un niño y la información biométrica y de salud están cubiertos por la Regla COPPA cuando se recopilan con otros datos personales.
4. La FTC obtuvo una orden contra el proveedor de tecnología educativa Edmodo, Inc. por recopilar datos personales de niños sin obtener el consentimiento de sus padres y utilizar esos datos para publicidad, en violación de la regla COPPA, y por subcontratar ilegalmente sus responsabilidades de cumplimiento de COPPA a las escuelas. Según la orden, Edmodo tiene prohibido, entre otras cosas, exigir a los estudiantes que entreguen más datos personales de los necesarios para participar en una actividad educativa en línea, lo cual es una novedad en una orden de la FTC. La orden propuesta también incluye una multa civil suspendida de $6 millones.

Órdenes sobre la regla de notificación de infracciones de salud:

1. La FTC tomó medidas coercitivas por primera vez bajo su Regla de notificación de infracciones de salud contra el proveedor de telesalud y descuentos en medicamentos recetados GoodRx Holdings Inc., por no notificar a los consumidores y a otras personas sobre sus divulgaciones no autorizadas de datos personales de los consumidores. información de salud a Facebook, Google y otras empresas En una orden propuesta, primera en su tipo, presentada por el DOJ en nombre de la FTC, GoodRx tiene prohibido compartir datos de salud de los usuarios con terceros

aplicables con fines publicitarios, y ha acordado pagar una multa civil de 1,5 millones de dólares por violar la regla.

2. La FTC acusó que el desarrollador de la aplicación de fertilidad Premom engañó a los usuarios al compartir su información personal confidencial con terceros, incluidas dos empresas con sede en China, reveló datos de salud confidenciales de los usuarios a AppsFlyer y Google, y no notificó a los consumidores sobre estas divulgaciones no autorizadas en violación de la Regla de Notificación de Infracciones de Salud. La orden, que se introdujo el 22 de junio de 2023, prohíbe al desarrollador de la aplicación, Easy Care Healthcare Corporation, compartir datos de salud personales de los usuarios con terceros con fines publicitarios, requiere que la aplicación obtenga el consentimiento de los usuarios antes de compartir datos de salud para cualquier otro propósito, y para informar a los consumidores cómo se utilizarán sus datos personales.

3. En el año fiscal 2023, la FTC buscó comentarios públicos sobre los cambios propuestos a la Regla de Notificación de Infracciones de Salud que incluyen aclarar la aplicabilidad de la regla a aplicaciones de salud y otras tecnologías similares. Desde la emisión de la norma, las aplicaciones de salud y otras tecnologías de salud directas al consumidor, como los rastreadores de actividad física, se han vuelto comunes. Los cambios propuestos a la regla se producen en un momento en que las prácticas comerciales y los desarrollos tecnológicos aumentan tanto la cantidad de datos de salud recopilados de los consumidores como el incentivo para que las empresas utilicen o divulguen esos datos confidenciales datos para marketing y otros fines. En abril de 2024, la Comisión votó para finalizar los cambios a la Regla de Notificación de Infracciones de Salud.

Declaración de política de información biométrica:

1. La FTC emitió una declaración de política advirtiendo que el uso cada vez mayor de información biométrica de los consumidores y tecnologías relacionadas, incluidas aquellas impulsadas por el aprendizaje automático, plantea importantes preocupaciones sobre la privacidad y la seguridad de los datos de los consumidores y el potencial de sesgo y discriminación. La información biométrica se refiere a datos que representan o describen rasgos, características o medidas físicas, biológicas o de comportamiento del cuerpo de una persona identificada o identificable o relacionados con él. La declaración de política advierte que las afirmaciones falsas o sin fundamento sobre la exactitud o eficacia de las tecnologías de información

biométrica o sobre la recopilación y el uso de información biométrica pueden violar la Ley de la FTC.

2. La FTC acusó a la empresa de pruebas genéticas 1Health.io Inc., anteriormente conocida como Vitagene, de dejar datos genéticos y de salud confidenciales sin protección, engañar a los consumidores sobre su capacidad para eliminar sus datos y cambiar su política de privacidad retroactivamente sin notificar ni obtener el consentimiento adecuadamente de consumidores cuyos datos la empresa ya había recopilado. Como parte de la orden final con la FTC, 1Health acordó pagar $75,000 y fortalecerá la protección de la información genética e instruirá a laboratorios contratados por terceros para que destruyan todas las muestras de ADN de los consumidores que hayan sido retenidas durante más de 180 días.

Órdenes de datos de salud:

1. La FTC finalizó una orden que prohíbe al servicio de asesoramiento en línea BetterHelp, Inc. compartir datos de salud de los consumidores, incluida información confidencial sobre problemas de salud mental, para publicidad. La orden también requiere que la compañía pague 7,8 millones de dólares a los consumidores para resolver los cargos de que reveló datos confidenciales de los consumidores a terceros como Facebook y Snapchat para publicidad después de prometer mantener dichos datos privados datos para marketing y otros fines. En abril de 2024, la Comisión votó para finalizar los cambios a la Regla de Notificación de Infracciones de Salud.

Privacidad de la salud:

1. La FTC y la Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos de EE. UU. advirtieron a los hospitales y proveedores de telesalud sobre los riesgos de privacidad y seguridad relacionados con el uso de tecnologías de seguimiento en línea integradas en sus sitios web o aplicaciones móviles que puede estar divulgando de forma inadmisible datos de salud personales sensibles de los consumidores a terceros. Las dos agencias enviaron una carta conjunta a aproximadamente 130 sistemas hospitalarios y proveedores de telesalud para alertarlos sobre los riesgos y preocupaciones con respecto al uso de tecnologías, como el píxel Meta/Facebook y Google Analytics, que pueden rastrear las actividades en línea de un usuario. Estas tecnologías de seguimiento recopilan información identificable sobre los usuarios, generalmente sin su conocimiento y de maneras que son difíciles de evitar para los usuarios, cuando los usuarios

interactúan con un sitio web o una aplicación móvil.

Orden de vigilancia ilegal:

1. La FTC acusó a la empresa de cámaras de seguridad para el hogar Ring, LLC de comprometer la privacidad de sus clientes al permitir que cualquier empleado o contratista acceda a los vídeos privados de los consumidores y de no implementar protecciones básicas de privacidad y seguridad, lo que permitió a los piratas informáticos tomar el control de cuentas, cámaras y vídeos de los consumidores. La orden judicial exige que Ring pague 5,8 millones de dólares y elimine productos de datos como datos, modelos y algoritmos derivados de vídeos que revisó ilegalmente. La orden también requiere que Ring implemente un programa de privacidad y seguridad con novedosas salvaguardias sobre la revisión humana de videos, así como otros controles de seguridad estrictos, como la autenticación multifactor para cuentas de empleados y clientes.

Órdenes de seguridad de datos:

1. La FTC finalizó una orden con el mercado de bebidas alcohólicas en línea Drizly, LLC y su director ejecutivo sobre fallas de seguridad de la compañía que, según la FTC, llevaron a una violación de datos que expuso la información personal de alrededor de 2,5 millones de consumidores. La FTC alegó que Drizly y su director ejecutivo fueron alertados sobre vulnerabilidades de seguridad dos años antes de la violación de 2020, pero no tomaron medidas para proteger los datos de los consumidores de los piratas informáticos a pesar de afirmar públicamente que contaban con protecciones de seguridad adecuadas. La orden de la FTC, entre otras cosas, exige que Drizly destruya cualquier dato personal que haya recopilado y que no sea necesario para proporcionar productos o servicios a los consumidores y debe abstenerse de recopilar o almacenar información personal a menos que sea necesario para fines específicos descritos.
2. La FTC finalizó su orden con el proveedor de tecnología educativa Chegg Inc. por sus prácticas descuidadas de seguridad de datos que expusieron información confidencial sobre millones de clientes y empleados de Chegg, incluidos números de Seguro Social, direcciones de correo electrónico y contraseñas. La orden de la FTC exige que Chegg implemente un programa integral de seguridad de la información, limite los datos que la empresa puede recopilar y retener, ofrezca a los

usuarios autenticación multifactor para proteger sus cuentas y permita a los usuarios solicitar acceso a sus datos y eliminarlos.

Datos del consumidor de preparación de impuestos:

1. La FTC utilizó su autoridad sobre delitos penales para advertir a cinco empresas preparadoras que podrían enfrentar sanciones civiles si utilizan o divulgan datos confidenciales, recopilados de los consumidores con el fin de preparar sus impuestos, para fines no relacionados, como publicidad, sin obtener primero el consentimiento de los consumidores. Al enviar un Aviso de sanciones, la agencia advierte a los destinatarios que podrían incurrir en sanciones civiles de hasta $50,120 por infracción si hacen un uso indebido de los datos personales de manera contraria a propósito original para el cual se recopiló esta información.

Órdenes de infracción de la Ley de Informe Justo de Crédito:

1. Proveedores de informes de antecedentes TruthFinder y Instant Checkmate aceptó una orden propuesta que les exigía pagar 5,8 millones de dólares para resolver los cargos de que engañaron a los consumidores sobre si tenían antecedentes penales y que las empresas violaron la Ley de Informe Justo de Crédito (FCRA, por sus siglas en inglés) al operar como agencias de informes de consumidores mientras, entre otras cosas al no garantizar la máxima precisión posible de sus informes de consumo. La orden propuesta también requiere que las empresas implementen un programa de monitoreo de la FCRA, entre otras disposiciones.

Anexo 3: Requisitos funcionales y no funcionales

Propuesta construida por [43]:

IDENTIFICACIÓN	Requisitos Funcionales (El sistema debería…)
RF01	DEBERÍA permitir que los participantes que comparten datos modifiquen los datos (flujos).
RF02	DEBE garantizar que las modificaciones de datos (flujo) sean consistentes con las condiciones de uso de los datos.
RF03	DEBERÍA permitir que un proveedor de datos interrumpa las actividades de procesamiento de datos en el lado del consumidor de datos.
RF04	PODRÍA permitir que un proveedor de datos ejecute operaciones en datos compartidos en el lado del consumidor de datos.
RF05	DEBE evitar intervenciones de terceros sin el consentimiento de los participantes en el intercambio de datos.
RF06	DEBE proporcionar notificaciones si el uso de datos no cumple con las condiciones de uso de datos.
RF07	PODRÍA permitir a los participantes del intercambio de datos negociar las condiciones de uso de estos.
RF08	PODRÍA proporcionar una interfaz gráfica de usuario para reducir las barreras para los no expertos.
RF09	DEBE proporcionar funciones para realizar un seguimiento de las actividades de procesamiento de datos y el linaje de datos en cualquier momento.
RF10	DEBE garantizar que las condiciones de uso de los datos sean accesibles para todos los participantes que comparten datos.
RF11	DEBERÍA proporcionar características para enriquecer cualquier dato con metadatos, al menos las condiciones de uso de los datos.
RF12	DEBE asignar un identificador único persistente en todo el sistema a cada conjunto de datos.
RF13	PODRÍA proporcionar características que mejoren la capacidad de descubrimiento de datos.
RF14	DEBE proporcionar mecanismos para garantizar la indisputabilidad de los hechos y acciones que ocurren.
RF15	DEBE incorporar mecanismos para autenticar y verificar la identidad de los participantes del intercambio de datos.
RF16	DEBE garantizar el acceso a los datos y metadatos únicamente por parte de actores autorizados, es decir, sistemas y usuarios.
RF17	DEBE hacer cumplir el manejo confidencial de los datos de acuerdo con las condiciones de uso de datos acordadas.

RF18	DEBE prohibir cambios a los datos por parte de un participante que comparte datos sin el consentimiento del proveedor de datos.
RF19	no DEBE eliminar ninguna referencia al origen de los datos sin el consentimiento explícito del proveedor de los datos.
RF20	PODRÍA implementar formatos de datos comunes para facilitar las transferencias de datos.
RF21	DEBE implementar vocabularios comunes para las condiciones de uso de datos.
RF22	DEBERÍA implementar protocolos comunes para compartir datos.
	Requisitos No Funcionales
	Intervenibilidad: Grado en el que un sistema, producto o componente evita el acceso no autorizado y/o modificación del programa informático o de los datos
	Seguridad: Grado en el que un producto o sistema protege la información y los datos para que las personas, productos u otros sistemas tengan un grado de acceso a los datos de acuerdo con sus tipos y niveles de autorización
	Interoperabilidad: Grado en el que dos o más sistemas, productos o componentes pueden intercambiar información y utilizar la información que se ha intercambiado.

Anexo 4: Ejecución de Guía para Empresas

1. Auditoría Inicial de Datos

1.1 Datos críticos:

- Clientes y proveedores, así como información financiera y operativa, serán objeto de un análisis exhaustivo para identificar vulnerabilidades y establecer controles adecuados.
- Empleados, información sensible y acceso a sistemas también serán evaluados para garantizar que se sigan las políticas de seguridad y se minimicen los riesgos asociados.
- Datos financieros como los balances, transacciones y proyecciones serán revisados para detectar posibles brechas de seguridad y asegurar la integridad de la información.
- Datos estratégicos como valores de mercado, análisis de competencia y planes de negocio se analizarán para proteger la información crítica que puede influir en la toma de decisiones estratégicas.

1.2 Clasificación de datos

Existirán tres niveles de sensibilidad: alta, media y baja, cada uno con protocolos específicos para su manejo y protección.

- Para nivel bajo: correo electrónico, nombres y apellidos y contraseña.
- Para nivel medio: historial de compras, y preferencias del cliente, así como información de contacto.
- Para nivel alto: datos financieros sensibles, información personal identificable y cualquier dato que pueda comprometer la seguridad de la empresa o de sus clientes.

2. **Cumplimiento Normativo**

Consideraremos la normativa vigente en materia de protección de datos, asegurando que todas las prácticas se alineen con las regulaciones locales e internacionales, como el GDPR y la LOPD y asignaremos un Responsable de Protección de datos que supervisará el cumplimiento de estas normativas y actuará como punto de contacto para cualquier consulta relacionada con la privacidad y la seguridad de la información.

3. **Políticas de Localización de datos**

3.1 Almacenamiento local y nube: Se establecerán para garantizar que los datos se almacenen y procesen en ubicaciones que cumplan con los requisitos legales aplicables, minimizando así el riesgo de violaciones de seguridad y asegurando la integridad de la información. Además, se implementarán medidas de cifrado y acceso restringido para proteger la información sensible, así como auditorías periódicas para evaluar la efectividad de estas políticas y realizar ajustes necesarios.

3.2 Requisitos de proveedores en la nube: Se evaluarán cuidadosamente los proveedores en función de su capacidad para cumplir con las normativas de seguridad y privacidad, asegurando que cuenten con certificaciones adecuadas y protocolos de protección de datos robustos. Asimismo, se establecerán acuerdos de nivel de servicio (SLA) que definan claramente las expectativas en cuanto a la disponibilidad y respuesta ante incidentes, garantizando así una colaboración efectiva y segura.

4. Medidas de Seguridad

4.1 Cifrado robusto y autenticación multifactor; se implementarán para salvaguardar el acceso a los sistemas críticos, minimizando el riesgo de brechas de seguridad y asegurando que solo el personal autorizado pueda acceder a la información confidencial.

4.2 Monitorización de accesos; se llevará a cabo de manera continua, permitiendo detectar actividades sospechosas y responder de forma proactiva ante posibles amenazas. Además, se realizarán auditorías periódicas para evaluar la efectividad de las medidas implementadas y ajustar las estrategias según sea necesario. Asimismo, se fomentará la capacitación constante del personal en materia de seguridad, asegurando que todos estén al tanto de las mejores prácticas y protocolos a seguir en caso de incidentes. Se establecerán canales de comunicación claros para

reportar cualquier irregularidad, garantizando una respuesta rápida y coordinada ante situaciones de emergencia. También se implementarán simulacros regulares para preparar al equipo ante posibles escenarios de crisis, fortaleciendo así la cultura de seguridad dentro de la organización. Se buscará la colaboración con expertos externos para enriquecer las estrategias de seguridad y asegurar que se estén utilizando las tecnologías más avanzadas disponibles en el mercado. Además, se realizará una evaluación periódica de los riesgos para identificar áreas de mejora y adaptar las medidas de seguridad a las necesidades cambiantes del entorno.

5. Gestión de Proveedores y Terceros

5.1 Evaluación de proveedores: se llevará a cabo un proceso riguroso que incluya la revisión de sus credenciales, historial de cumplimiento y capacidad para cumplir con los estándares de seguridad establecidos.

5.2 Acuerdos de procesamiento de datos: se establecerán acuerdos claros que definan las responsabilidades de cada parte en el manejo de datos sensibles, garantizando así la protección de la información y el cumplimiento de las normativas vigentes. Solicitando que los proveedores cumplan con auditorías regulares y reporten cualquier incidente de seguridad que pueda afectar la integridad de los datos.

6. Políticas de Accedo y Control

6.1 Acceso basados en roles (RBAC): se implementará un sistema que limite el acceso a la información según las funciones y responsabilidades de cada usuario, asegurando que solo aquellos con la autorización adecuada puedan acceder a datos críticos.

6.2 Privacidad por diseño: se integrará en el desarrollo de nuevos sistemas y procesos, garantizando que la protección de la privacidad sea una consideración fundamental desde las etapas iniciales.

7. Plan de Respuestas ante Incidentes

7.1 Plan de contingencia ante fugas de datos: se establecerán protocolos claros para la identificación, contención y notificación de incidentes, así como medidas para mitigar el impacto en los afectados y restaurar la seguridad de la información.

7.2 Notificación de incidentes: se informará a las partes interesadas y a las autoridades pertinentes de manera oportuna, cumpliendo con las regulaciones aplicables y asegurando la transparencia en el manejo de la situación.

7.3 Evaluación post-incidente: se llevará a cabo un análisis exhaustivo de cada incidente para identificar las causas raíz y mejorar los protocolos existentes, con el fin de prevenir futuros problemas y fortalecer la resiliencia organizacional.

8. Capacitación del Personal

8.1 Capacitación en seguridad de datos: se implementarán programas de formación continua para todo el personal, asegurando que estén al tanto de las mejores prácticas y procedimientos actualizados en la protección de la información. Además, se fomentará una cultura de seguridad donde cada empleado se sienta responsable de la protección de los datos y pueda reportar cualquier anomalía de manera inmediata.

8.2 Concienciación sobre la protección de datos: se llevarán a cabo campañas de sensibilización periódicas que informen sobre la importancia de la privacidad y las implicaciones legales de su incumplimiento. Estas iniciativas incluirán talleres interactivos y materiales informativos accesibles para todos los niveles de la organización.

9. Monitoreo y Auditoría Continua

9.1 Auditorias periódicas: se realizarán para evaluar la efectividad de las medidas implementadas y detectar posibles vulnerabilidades. Esto permitirá ajustar las estrategias de seguridad según sea necesario y garantizar que se mantenga un alto estándar de protección de datos en todo momento.

9.2 Ajustes y actualizaciones: se llevarán a cabo de forma regular para incorporar las últimas tecnologías y mejores prácticas en el ámbito de la ciberseguridad, asegurando así que la organización se mantenga a la vanguardia en la defensa contra amenazas emergentes.

10. Beneficios y Conclusiones

10.1 Protección de la empresa y clientes: la implementación de estas medidas no solo salvaguardará la información sensible, sino que también fortalecerá la confianza de los clientes en la organización, promoviendo relaciones comerciales más sólidas y duraderas.

10.2 Confianza de los clientes: la confianza de los clientes se verá reflejada en un aumento de la lealtad y en la disposición a recomendar nuestros servicios, lo que a su vez impulsará el crecimiento y la reputación de la empresa en el mercado.

10.3 Cumplimiento regulatorio: el cumplimiento de las normativas vigentes es esencial para evitar sanciones y mantener la integridad de la organización, lo que permitirá operar con mayor tranquilidad y seguridad en un entorno cada vez más regulado.